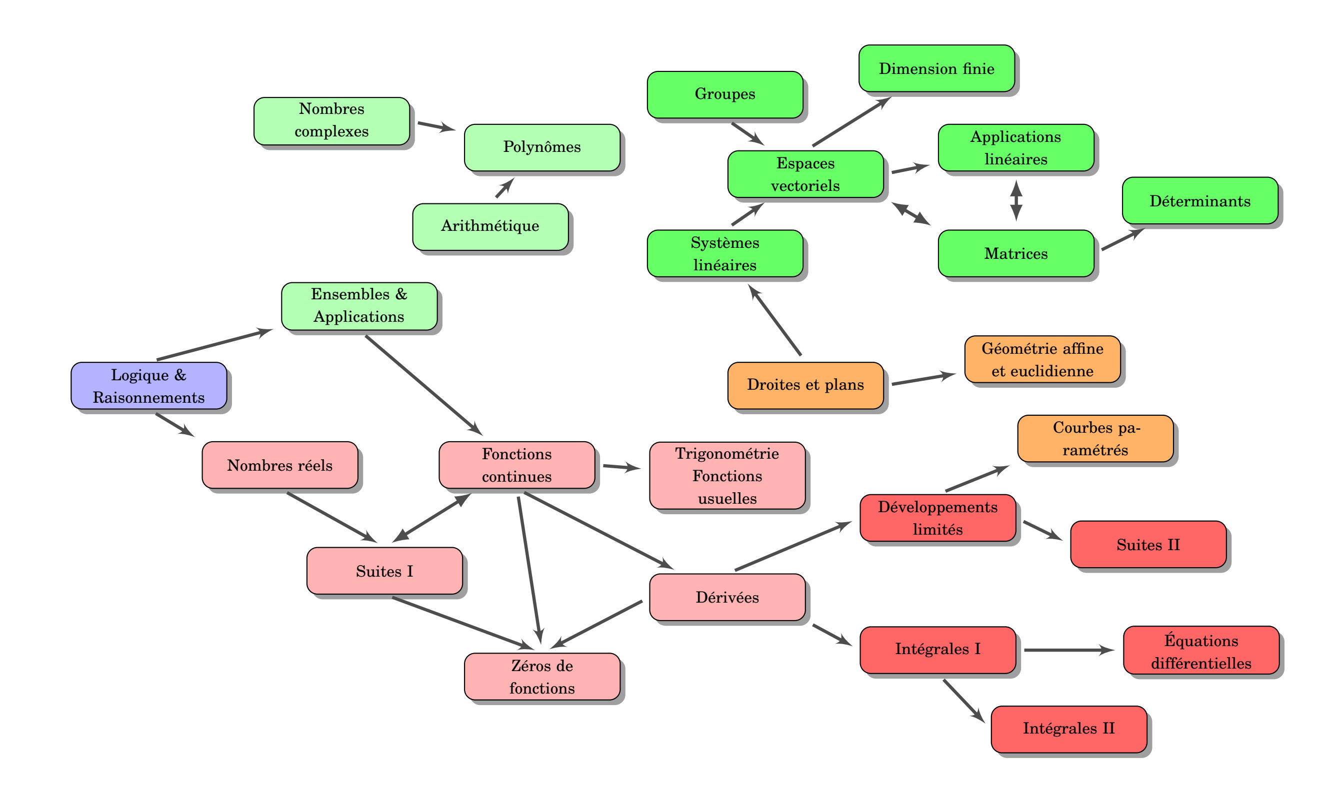
Cours de mathématiques
Première année





Sommaire


Nombres complexes
Polynômes
Arithmétique
Groupes
Dimension finie
Espaces vectoriels
Applications linéaires
Systèmes linéaires
Matrices
Déterminants
Ensembles & Applications
Logique & Raisonnements
Droites et plans
Géométrie affine et euclidienne
Nombres réels
Fonctions continues
Trigonométrie Fonctions usuelles
Courbes paramétrés
Développements limités
Suites II
Suites I
Dérivées
Intégrales I
Équations différentielles
Zéros de fonctions
Intégrales II



1 Logique et raisonnements

Vidéo ■ partie 1. Logique
Vidéo ■ partie 2. Raisonnements
Exercices ♦ Logique, ensembles, raisonnements

Quelques motivations

- Il est important d'avoir un ***langage rigoureux***. La langue française est souvent ambigüe. Prenons l'exemple de la conjonction « *ou* » ; au restaurant « *fromage ou dessert* » signifie l'un ou l'autre mais pas les deux. Par contre si dans un jeu de carte on cherche « *les as ou les cœurs* » alors il ne faut pas exclure l'as de cœur. Autre exemple : que répondre à la question « *As-tu* 10 *euros en poche ?* » si l'on dispose de 15 euros ?
- Il y a des notions difficiles à expliquer avec des mots : par exemple la continuité d'une fonction est souvent expliquée par « *on trace le graphe sans lever le crayon* ». Il est clair que c'est une définition peu satisfaisante. Voici la définition mathématique de la continuité d'une fonction $f : I \to \mathbb{R}$ en un point $x_0 \in I$:

$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad (|x - x_0| < \delta \implies |f(x) - f(x_0)| < \varepsilon).$$

  C'est le but de ce chapitre de rendre cette ligne plus claire ! C'est la ***logique***.
- Enfin les mathématiques tentent de ***distinguer le vrai du faux***. Par exemple « *Est-ce qu'une augmentation de* 20%*, puis de* 30% *est plus intéressante qu'une augmentation de* 50% *?* ». Vous pouvez penser « *oui* » ou « *non* », mais pour en être sûr il faut suivre une démarche logique qui mène à la conclusion. Cette démarche doit être convaincante pour vous mais aussi pour les autres. On parle de ***raisonnement***.

Les mathématiques sont un langage pour s'exprimer rigoureusement, adapté aux phénomènes complexes, qui rend les calculs exacts et vérifiables. Le raisonnement est le moyen de valider — ou d'infirmer — une hypothèse et de l'expliquer à autrui.

1. Logique

1.1. Assertions

Une ***assertion*** est une phrase soit vraie, soit fausse, pas les deux en même temps.
Exemples :
- « *Il pleut.* »
- « *Je suis plus grand que toi.* »
- « $2 + 2 = 4$ »

- « $2 \times 3 = 7$ »
- « *Pour tout* $x \in \mathbb{R}$, *on a* $x^2 \geqslant 0$. »
- « *Pour tout* $z \in \mathbb{C}$, *on a* $|z| = 1$. »

Si P est une assertion et Q est une autre assertion, nous allons définir de nouvelles assertions construites à partir de P et de Q.

L'opérateur logique « *et* »

L'assertion « P **et** Q » est vraie si P est vraie et Q est vraie. L'assertion « P *et* Q » est fausse sinon. On résume ceci en une ***table de vérité*** :

$P \setminus Q$	V	F
V	V	F
F	F	F

FIGURE 1.1 – Table de vérité de « P *et* Q »

Par exemple si P est l'assertion « *Cette carte est un as* » et Q l'assertion « *Cette carte est cœur* » alors l'assertion « P *et* Q » est vraie si la carte est l'as de cœur et est fausse pour toute autre carte.

L'opérateur logique « *ou* »

L'assertion « P **ou** Q » est vraie si l'une des deux assertions P ou Q est vraie. L'assertion « P *ou* Q » est fausse si les deux assertions P et Q sont fausses.
On reprend ceci dans la table de vérité :

$P \setminus Q$	V	F
V	V	V
F	V	F

FIGURE 1.2 – Table de vérité de « P *ou* Q »

Si P est l'assertion « *Cette carte est un as* » et Q l'assertion « *Cette carte est cœur* » alors l'assertion « P *ou* Q » est vraie si la carte est un as ou bien un cœur (en particulier elle est vraie pour l'as de cœur).

Remarque

Pour définir les opérateurs « *ou* », « *et* » on fait appel à une phrase en français utilisant les mots *ou*, *et* ! Les tables de vérités permettent d'éviter ce problème.

La négation « *non* »

L'assertion « **non** P » est vraie si P est fausse, et fausse si P est vraie.

P	V	F
non P	F	V

FIGURE 1.3 – Table de vérité de « *non* P »

L'implication $\Longrightarrow$

La définition mathématique est la suivante :

L'assertion « *(non P) ou Q* » est notée « $P \Longrightarrow Q$ ».

Sa table de vérité est donc la suivante :

$P \setminus Q$	V	F
V	V	F
F	V	V

FIGURE 1.4 – Table de vérité de « $P \Longrightarrow Q$ »

L'assertion « $P \Longrightarrow Q$ » se lit en français « *P implique Q* ».
Elle se lit souvent aussi « *si P est vraie alors Q est vraie* » ou « *si P alors Q* ».
Par exemple :

- « $0 \leqslant x \leqslant 25 \Longrightarrow \sqrt{x} \leqslant 5$ » est vraie (prendre la racine carrée).
- « $x \in]-\infty, -4[\Longrightarrow x^2 + 3x - 4 > 0$ » est vraie (étudier le binôme).
- « $\sin(\theta) = 0 \Longrightarrow \theta = 0$ » est fausse (regarder pour $\theta = 2\pi$ par exemple).
- « $2 + 2 = 5 \Longrightarrow \sqrt{2} = 2$ » est vraie ! Eh oui, si P est fausse alors l'assertion « $P \Longrightarrow Q$ » est toujours vraie.

L'équivalence $\Longleftrightarrow$

L'***équivalence*** est définie par :

« $P \Longleftrightarrow Q$ » est l'assertion « $(P \Longrightarrow Q)$ *et* $(Q \Longrightarrow P)$ ».

On dira « *P est équivalent à Q* » ou « *P équivaut à Q* » ou « *P si et seulement si Q* ». Cette assertion est vraie lorsque P et Q sont vraies ou lorsque P et Q sont fausses. La table de vérité est :

$P \setminus Q$	V	F
V	V	F
F	F	V

FIGURE 1.5 – Table de vérité de « $P \Longleftrightarrow Q$ »

Exemples :

- Pour $x, x' \in \mathbb{R}$, l'équivalence « $x \cdot x' = 0 \Longleftrightarrow (x = 0$ *ou* $x' = 0)$ » est vraie.
- Voici une équivalence *toujours fausse* (quelque soit l'assertion P) : « $P \Longleftrightarrow$ *non*(P) ».

On s'intéresse davantage aux assertions vraies qu'aux fausses, aussi dans la pratique et en dehors de ce chapitre on écrira « $P \Longleftrightarrow Q$ » ou « $P \Longrightarrow Q$ » uniquement lorsque ce sont des assertions vraies. Par exemple si l'on écrit « $P \Longleftrightarrow Q$ » cela sous-entend « $P \Longleftrightarrow Q$ *est vraie* ». Attention rien ne dit que P et Q soient vraies. Cela signifie que P et Q sont vraies en même temps ou fausses en même temps.

Proposition 1

Soient P,Q,R trois assertions. Nous avons les équivalences (vraies) suivantes :

1. $P \iff non(non(P))$
2. $(P\ et\ Q) \iff (Q\ et\ P)$
3. $(P\ ou\ Q) \iff (Q\ ou\ P)$
4. $non(P\ et\ Q) \iff (non\ P)\ ou\ (non\ Q)$
5. $non(P\ ou\ Q) \iff (non\ P)\ et\ (non\ Q)$
6. $\big(P\ et\ (Q\ ou\ R)\big) \iff (P\ et\ Q)\ ou\ (P\ et\ R)$
7. $\big(P\ ou\ (Q\ et\ R)\big) \iff (P\ ou\ Q)\ et\ (P\ ou\ R)$
8. « $P \implies Q$ » $\iff$ « $non(Q) \implies non(P)$ »

Démonstration

Voici des exemples de démonstrations :

4. Il suffit de comparer les deux assertions « $non(P\ et\ Q)$ » et « $(non\ P)\ ou\ (non\ Q)$ » pour toutes les valeurs possibles de P et Q. Par exemple si P est vrai et Q est vrai alors « $P\ et\ Q$ » est vrai donc « $non(P\ et\ Q)$ » est faux ; d'autre part (non P) est faux, (non Q) est faux donc « $(non\ P)\ ou\ (non\ Q)$ » est faux. Ainsi dans ce premier cas les assertions sont toutes les deux fausses. On dresse ainsi les deux tables de vérités et comme elles sont égales les deux assertions sont équivalentes.

$P \setminus Q$	V	F
V	F	V
F	V	V

FIGURE 1.6 – Tables de vérité de « $non(P\ et\ Q)$ » et de « $(non\ P)\ ou\ (non\ Q)$ »

6. On fait la même chose mais il y a trois variables : P, Q, R. On compare donc les tables de vérité d'abord dans le cas où P est vrai (à gauche), puis dans le cas où P est faux (à droite). Dans les deux cas les deux assertions « $\big(P\ et\ (Q\ ou\ R)\big)$ » et « $(P\ et\ Q)\ ou\ (P\ et\ R)$ » ont la même table de vérité donc les assertions sont équivalentes.

$Q \setminus R$	V	F
V	V	V
F	V	F

$Q \setminus R$	V	F
V	F	F
F	F	F

8. Par définition, l'implication « $P \implies Q$ » est l'assertion « $(non\ P)\ ou\ Q$ ».
Donc l'implication « $non(Q) \implies non(P)$ » est équivalente à « $non(non(Q))\ ou\ non(P)$ » qui équivaut encore à « $Q\ ou\ non(P)$ » et donc est équivalente à « $P \implies Q$ ». On aurait aussi pu encore une fois dresser les deux tables de vérité et voir quelles sont égales.

1.2. Quantificateurs

Le quantificateur ∀ : « *pour tout* »

Une assertion P peut dépendre d'un paramètre x, par exemple « $x^2 \geqslant 1$ », l'assertion $P(x)$ est vraie ou fausse selon la valeur de x.

L'assertion

$$\forall x \in E \quad P(x)$$

est une assertion vraie lorsque les assertions $P(x)$ sont vraies pour tous les éléments x de l'ensemble E.
On lit « *Pour tout x appartenant à E, $P(x)$* », sous-entendu « *Pour tout x appartenant à E, $P(x)$ est vraie* ».
Par exemple :

- « $\forall x \in [1, +\infty[\quad (x^2 \geqslant 1)$ » est une assertion vraie.
- « $\forall x \in \mathbb{R} \quad (x^2 \geqslant 1)$ » est une assertion fausse.
- « $\forall n \in \mathbb{N} \quad n(n+1)$ *est divisible par* 2 » est vraie.

Le quantificateur ∃ : « *il existe* »

L'assertion

$$\exists x \in E \quad P(x)$$

est une assertion vraie lorsque l'on peut trouver au moins un x de E pour lequel $P(x)$ est vraie. On lit « *il existe x appartenant à E tel que $P(x)$ (soit vraie)* ».
Par exemple :

- « $\exists x \in \mathbb{R} \quad (x(x-1) < 0)$ » est vraie (par exemple $x = \frac{1}{2}$ vérifie bien la propriété).
- « $\exists n \in \mathbb{N} \quad n^2 - n > n$ » est vraie (il y a plein de choix, par exemple $n = 3$ convient, mais aussi $n = 10$ ou même $n = 100$, un seul suffit pour dire que l'assertion est vraie).
- « $\exists x \in \mathbb{R} \quad (x^2 = -1)$ » est fausse (aucun réel au carré ne donnera un nombre négatif).

La négation des quantificateurs

La négation de « $\forall x \in E \quad P(x)$ » est « $\exists x \in E \quad$ *non* $P(x)$ » .

Par exemple la négation de « $\forall x \in [1, +\infty[\quad (x^2 \geqslant 1)$ » est l'assertion « $\exists x \in [1, +\infty[\quad (x^2 < 1)$ ». En effet la négation de $x^2 \geqslant 1$ est non$(x^2 \geqslant 1)$ mais s'écrit plus simplement $x^2 < 1$.

La négation de « $\exists x \in E \quad P(x)$ » est « $\forall x \in E \quad$ *non* $P(x)$ ».

Voici des exemples :

- La négation de « $\exists z \in \mathbb{C} \quad (z^2 + z + 1 = 0)$ » est « $\forall z \in \mathbb{C} \quad (z^2 + z + 1 \neq 0)$ ».
- La négation de « $\forall x \in \mathbb{R} \quad (x + 1 \in \mathbb{Z})$ » est « $\exists x \in \mathbb{R} \quad (x + 1 \notin \mathbb{Z})$ ».
- Ce n'est pas plus difficile d'écrire la négation de phrases complexes. Pour l'assertion :

$$\forall x \in \mathbb{R} \quad \exists y > 0 \quad (x + y > 10)$$

sa négation est

$$\exists x \in \mathbb{R} \quad \forall y > 0 \quad (x + y \leqslant 10).$$

Remarques

L'ordre des quantificateurs est très important. Par exemple les deux phrases logiques

$$\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R} \quad (x + y > 0) \qquad \text{et} \qquad \exists y \in \mathbb{R} \quad \forall x \in \mathbb{R} \quad (x + y > 0).$$

sont différentes. La première est vraie, la seconde est fausse. En effet une phrase logique se lit de gauche à droite, ainsi la première phrase affirme « *Pour tout réel x, il existe un réel y (qui peut donc*

dépendre de x) tel que $x+y>0$. » (par exemple on peut prendre $y=x+1$). C'est donc une phrase vraie. Par contre la deuxième se lit : « *Il existe un réel y, tel que pour tout réel x,* $x+y>0$. » Cette phrase est fausse, cela ne peut pas être le même y qui convient pour tous les x !
On retrouve la même différence dans les phrases en français suivantes. Voici une phrase vraie « *Pour toute personne, il existe un numéro de téléphone* », bien sûr le numéro dépend de la personne. Par contre cette phrase est fausse : « *Il existe un numéro, pour toutes les personnes* ». Ce serait le même numéro pour tout le monde !

Terminons avec d'autres remarques.

- Quand on écrit « $\exists x \in \mathbb{R} \quad (f(x)=0)$ » cela signifie juste qu'il existe un réel pour lequel f s'annule. Rien ne dit que ce x est unique. Dans un premier temps vous pouvez lire la phrase ainsi : « *il existe* au moins *un réel x tel que* $f(x)=0$ ». Afin de préciser que f s'annule en une unique valeur, on rajoute un point d'exclamation :
$$\exists! x \in \mathbb{R} \quad (f(x)=0).$$
- Pour la négation d'une phrase logique, il n'est pas nécessaire de savoir si la phrase est fausse ou vraie. Le procédé est algorithmique : on change le « *pour tout* » en « *il existe* » et inversement, puis on prend la négation de l'assertion P.
- Pour la négation d'une proposition, il faut être précis : la négation de l'inégalité stricte « $<$ » est l'inégalité large « $\geqslant$ », et inversement.
- Les quantificateurs ne sont pas des abréviations. Soit vous écrivez une phrase en français : « *Pour tout réel x, si* $f(x)=1$ *alors* $x\geqslant 0$. » , soit vous écrivez la phrase logique :
$$\forall x \in \mathbb{R} \quad (f(x)=1 \implies x \geqslant 0).$$
Mais surtout n'écrivez pas « $\forall x$ *réel, si* $f(x)=1 \implies x$ *positif ou nul* ». Enfin, pour passer d'une ligne à l'autre d'un raisonnement, préférez plutôt « *donc* » à « $\implies$ ».
- Il est défendu d'écrire $\nexists, \not\Longrightarrow$. Ces symboles n'existent pas !

Mini-exercices

1. Écrire la table de vérité du « *ou exclusif* ». (C'est le *ou* dans la phrase « *fromage ou dessert* », l'un ou l'autre mais pas les deux.)
2. Écrire la table de vérité de « *non (P et Q)* ». Que remarquez vous ?
3. Écrire la négation de « $P \implies Q$ ».
4. Démontrer les assertions restantes de la proposition 1.
5. Écrire la négation de « $\big(P$ *et* $(Q$ *ou* $R)\big)$ ».
6. Écrire à l'aide des quantificateurs la phrase suivante : « *Pour tout nombre réel, son carré est positif* ». Puis écrire la négation.
7. Mêmes questions avec les phrases : « *Pour chaque réel, je peux trouver un entier relatif tel que leur produit soit strictement plus grand que* 1 ». Puis « *Pour tout entier n, il existe un unique réel x tel que* $\exp(x)$ *égale n* ».

2. Raisonnements

Voici des méthodes classiques de raisonnements.

2.1. Raisonnement direct

On veut montrer que l'assertion « $P \implies Q$ » est vraie. On suppose que P est vraie et on montre qu'alors Q est vraie. C'est la méthode à laquelle vous êtes le plus habitué.

Exemple 1

Montrer que si $a, b \in \mathbb{Q}$ alors $a + b \in \mathbb{Q}$.

Démonstration

Prenons $a \in \mathbb{Q}$, $b \in \mathbb{Q}$. Rappelons que les rationnels $\mathbb{Q}$ sont l'ensemble des réels s'écrivant $\frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$.
Alors $a = \frac{p}{q}$ pour un certain $p \in \mathbb{Z}$ et un certain $q \in \mathbb{N}^*$. De même $b = \frac{p'}{q'}$ avec $p' \in \mathbb{Z}$ et $q' \in \mathbb{N}^*$. Maintenant

$$a + b = \frac{p}{q} + \frac{p'}{q'} = \frac{pq' + qp'}{qq'}.$$

Or le numérateur $pq' + qp'$ est bien un élément de $\mathbb{Z}$; le dénominateur qq' est lui un élément de $\mathbb{N}^*$. Donc $a + b$ s'écrit bien de la forme $a + b = \frac{p''}{q''}$ avec $p'' \in \mathbb{Z}$, $q'' \in \mathbb{N}^*$. Ainsi $a + b \in \mathbb{Q}$.

2.2. Cas par cas

Si l'on souhaite vérifier une assertion $P(x)$ pour tous les x dans un ensemble E, on montre l'assertion pour les x dans une partie A de E, puis pour les x n'appartenant pas à A. C'est la méthode de ***disjonction*** ou du ***cas par cas***.

Exemple 2

Montrer que pour tout $x \in \mathbb{R}$, $|x - 1| \leqslant x^2 - x + 1$.

Démonstration

Soit $x \in \mathbb{R}$. Nous distinguons deux cas.
Premier cas : $x \geqslant 1$. Alors $|x - 1| = x - 1$. Calculons alors $x^2 - x + 1 - |x - 1|$.

$$\begin{aligned} x^2 - x + 1 - |x - 1| &= x^2 - x + 1 - (x - 1) \\ &= x^2 - 2x + 2 \\ &= (x - 1)^2 + 1 \geqslant 0. \end{aligned}$$

Ainsi $x^2 - x + 1 - |x - 1| \geqslant 0$ et donc $x^2 - x + 1 \geqslant |x - 1|$.
Deuxième cas : $x < 1$. Alors $|x - 1| = -(x - 1)$. Nous obtenons $x^2 - x + 1 - |x - 1| = x^2 - x + 1 + (x - 1) = x^2 \geqslant 0$. Et donc $x^2 - x + 1 \geqslant |x - 1|$.
Conclusion. Dans tous les cas $|x - 1| \leqslant x^2 - x + 1$.

2.3. Contraposée

Le raisonnement par ***contraposition*** est basé sur l'équivalence suivante (voir la proposition 1) :

L'assertion « $P \implies Q$ » est équivalente à « $non(Q) \implies non(P)$ ».

Donc si l'on souhaite montrer l'assertion « $P \implies Q$ », on montre en fait que si non(Q) est vraie alors non(P) est vraie.

Exemple 3

Soit $n \in \mathbb{N}$. Montrer que si n^2 est pair alors n est pair.

Démonstration

Nous supposons que n n'est pas pair. Nous voulons montrer qu'alors n^2 n'est pas pair. Comme n n'est pas pair, il est impair et donc il existe $k \in \mathbb{N}$ tel que $n = 2k+1$. Alors $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2\ell+1$ avec $\ell = 2k^2+2k \in \mathbb{N}$. Et donc n^2 est impair.

Conclusion : nous avons montré que si n est impair alors n^2 est impair. Par contraposition ceci est équivalent à : si n^2 est pair alors n est pair.

2.4. Absurde

Le ***raisonnement par l'absurde*** pour montrer « $P \implies Q$ » repose sur le principe suivant : on suppose à la fois que P est vraie et que Q est fausse et on cherche une contradiction. Ainsi si P est vraie alors Q doit être vraie et donc « $P \implies Q$ » est vraie.

Exemple 4

Soient $a, b \geqslant 0$. Montrer que si $\frac{a}{1+b} = \frac{b}{1+a}$ alors $a = b$.

Démonstration

Nous raisonnons par l'absurde en supposant que $\frac{a}{1+b} = \frac{b}{1+a}$ **et** $a \neq b$. Comme $\frac{a}{1+b} = \frac{b}{1+a}$ alors $a(1+a) = b(1+b)$ donc $a + a^2 = b + b^2$ d'où $a^2 - b^2 = b - a$. Cela conduit à $(a-b)(a+b) = -(a-b)$. Comme $a \neq b$ alors $a - b \neq 0$ et donc en divisant par $a - b$ on obtient $a + b = -1$. La somme de deux nombres positifs ne peut être négative. Nous obtenons une contradiction.

Conclusion : si $\frac{a}{1+b} = \frac{b}{1+a}$ alors $a = b$.

Dans la pratique, on peut choisir indifféremment entre un raisonnement par contraposition ou par l'absurde. Attention cependant de bien écrire quel type de raisonnement vous choisissez et surtout de ne pas changer en cours de rédaction !

2.5. Contre-exemple

Si l'on veut montrer qu'une assertion du type « $\forall x \in E \quad P(x)$ » est vraie alors pour chaque x de E il faut montrer que $P(x)$ est vraie. Par contre pour montrer que cette assertion est fausse alors il suffit de trouver $x \in E$ tel que $P(x)$ soit fausse. (Rappelez-vous la négation de « $\forall x \in E \quad P(x)$ » est « $\exists x \in E \quad \textit{non } P(x)$ »). Trouver un tel x c'est trouver un ***contre-exemple*** à l'assertion « $\forall x \in E \quad P(x)$ ».

Exemple 5

Montrer que l'assertion suivante est fausse « *Tout entier positif est somme de trois carrés* ».
(Les carrés sont les 0^2, 1^2, 2^2, 3^2,... Par exemple $6 = 2^2 + 1^2 + 1^2$.)

Démonstration

Un contre-exemple est 7 : les carrés inférieurs à 7 sont 0, 1, 4 mais avec trois de ces nombres on ne peut faire 7.

2.6. Récurrence

Le ***principe de récurrence*** permet de montrer qu'une assertion $P(n)$, dépendant de n, est vraie pour tout $n \in \mathbb{N}$. La démonstration par récurrence se déroule en trois étapes : lors de

l'***initialisation*** on prouve $P(0)$. Pour l'étape d'***hérédité***, on suppose $n \geqslant 0$ donné avec $P(n)$ vraie, et on démontre alors que l'assertion $P(n+1)$ au rang suivant est vraie. Enfin dans la ***conclusion***, on rappelle que par le principe de récurrence $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Exemple 6

Montrer que pour tout $n \in \mathbb{N}$, $2^n > n$.

Démonstration

Pour $n \geqslant 0$, notons $P(n)$ l'assertion suivante :

$$2^n > n.$$

Nous allons démontrer par récurrence que $P(n)$ est vraie pour tout $n \geqslant 0$.

Initialisation. Pour $n = 0$ nous avons $2^0 = 1 > 0$. Donc $P(0)$ est vraie.

Hérédité. Fixons $n \geqslant 0$. Supposons que $P(n)$ soit vraie. Nous allons montrer que $P(n+1)$ est vraie.

$$\begin{aligned} 2^{n+1} &= 2^n + 2^n \\ &> n + 2^n \qquad \text{car par } P(n) \text{ nous savons } 2^n > n, \\ &> n + 1 \qquad \text{car } 2^n \geqslant 1. \end{aligned}$$

Donc $P(n+1)$ est vraie.

Conclusion. Par le principe de récurrence $P(n)$ est vraie pour tout $n \geqslant 0$, c'est-à-dire $2^n > n$ pour tout $n \geqslant 0$.

Remarques :

- La rédaction d'une récurrence est assez rigide. Respectez scrupuleusement la rédaction proposée : donnez un nom à l'assertion que vous souhaitez montrer (ici $P(n)$), respectez les trois étapes (même si souvent l'étape d'initialisation est très facile). En particulier méditez et conservez la première ligne de l'hérédité « Fixons $n \geqslant 0$. Supposons que $P(n)$ soit vraie. Nous allons montrer que $P(n+1)$ est vraie. »
- Si on doit démontrer qu'une propriété est vraie pour tout $n \geqslant n_0$, alors on commence l'initialisation au rang n_0.
- Le principe de récurrence est basé sur la construction de $\mathbb{N}$. En effet un des axiomes pour définir $\mathbb{N}$ est le suivant : « *Soit A une partie de $\mathbb{N}$ qui contient 0 et telle que si $n \in A$ alors $n+1 \in A$. Alors $A = \mathbb{N}$* ».

Mini-exercices

1. (Raisonnement direct) Soient $a, b \in \mathbb{R}_+$. Montrer que si $a \leqslant b$ alors $a \leqslant \frac{a+b}{2} \leqslant b$ et $a \leqslant \sqrt{ab} \leqslant b$.
2. (Cas par cas) Montrer que pour tout $n \in \mathbb{N}$, $n(n+1)$ est divisible par 2 (distinguer les n pairs des n impairs).
3. (Contraposée ou absurde) Soient $a, b \in \mathbb{Z}$. Montrer que si $b \neq 0$ alors $a + b\sqrt{2} \notin \mathbb{Q}$. (On utilisera que $\sqrt{2} \notin \mathbb{Q}$.)
4. (Absurde) Soit $n \in \mathbb{N}^*$. Montrer que $\sqrt{n^2+1}$ n'est pas un entier.
5. (Contre-exemple) Est-ce que pour tout $x \in \mathbb{R}$ on a $x < 2 \implies x^2 < 4$?

6. (Récurrence) Montrer que pour tout $n \geqslant 1$, $1+2+\cdots+n = \frac{n(n+1)}{2}$.
7. (Récurrence) Fixons un réel $x \geqslant 0$. Montrer que pour tout entier $n \geqslant 1$, $(1+x)^n \geqslant 1+nx$.

Auteurs

Arnaud Bodin
Benjamin Boutin
Pascal Romon



2 Ensembles et applications

Vidéo ■ partie 1. Ensembles
Vidéo ■ partie 2. Applications
Vidéo ■ partie 3. Injection, surjection, bijection
Vidéo ■ partie 4. Ensembles finis
Vidéo ■ partie 5. Relation d'équivalence
Exercices ♦ Logique, ensembles, raisonnements
Exercices ♦ Injection, surjection, bijection
Exercices ♦ Dénombrement
Exercices ♦ Relation d'équivalence, relation d'ordre

Motivations

Au début du XXe siècle le professeur Frege peaufinait la rédaction du second tome d'un ouvrage qui souhaitait refonder les mathématiques sur des bases logiques. Il reçut une lettre d'un tout jeune mathématicien : « *J'ai bien lu votre premier livre. Malheureusement vous supposez qu'il existe un ensemble qui contient tous les ensembles. Un tel ensemble ne peut exister.* » S'ensuit une démonstration de deux lignes. Tout le travail de Frege s'écroulait et il ne s'en remettra jamais. Le jeune Russell deviendra l'un des plus grands logiciens et philosophes de sont temps. Il obtient le prix Nobel de littérature en 1950.

Voici le « paradoxe de Russell » pour montrer que l'ensemble de tous les ensembles ne peut exister. C'est très bref, mais difficile à appréhender. Par l'absurde, supposons qu'un tel ensemble $\mathscr{E}$ contenant tous les ensembles existe. Considérons

$$F = \left\{ E \in \mathscr{E} \mid E \notin E \right\}.$$

Expliquons l'écriture $E \notin E$: le E de gauche est considéré comme un élément, en effet l'ensemble $\mathscr{E}$ est l'ensemble de tous les ensembles et E est un élément de cet ensemble ; le E de droite est considéré comme un ensemble, en effet les élément de $\mathscr{E}$ sont des ensembles ! On peut donc s'interroger si l'élément E appartient à l'ensemble E. Si non, alors par définition on met E dans l'ensemble F.

La contradiction arrive lorsque l'on se pose la question suivante : a-t-on $F \in F$ ou $F \notin F$? L'une des deux affirmation doit être vraie. Et pourtant :

- Si $F \in F$ alors par définition de F, F est l'un des ensembles E tel que $F \notin F$. Ce qui est contradictoire.
- Si $F \notin F$ alors F vérifie bien la propriété définissant F donc $F \in F$! Encore contradictoire.

Aucun des cas n'est possible. On en déduit qu'il ne peut exister un tel ensemble $\mathscr{E}$ contenant tous les ensembles.
Ce paradoxe a été popularisé par l'énigme suivante : « *Dans une ville, le barbier rase tous ceux qui ne se rasent pas eux-mêmes. Qui rase le barbier ?* » La seule réponse valable est qu'une telle situation ne peut exister.

Ne vous inquiétez pas, Russell et d'autres ont fondé la logique et les ensembles sur des bases solides. Cependant il n'est pas possible dans ce cours de tout redéfinir. Heureusement, vous connaissez déjà quelques ensembles :

- l'ensemble des entiers naturels $\mathbb{N} = \{0,1,2,3,\dots\}$.
- l'ensemble des entiers relatifs $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$.
- l'ensemble des rationnels $\mathbb{Q} = \left\{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N}\setminus\{0\}\right\}$.
- l'ensemble des réels $\mathbb{R}$, par exemple $1, \sqrt{2}, \pi, \ln(2),\dots$
- l'ensemble des nombres complexes $\mathbb{C}$.

Nous allons essayer de voir les propriétés des ensembles, sans s'attacher à un exemple particulier. Vous vous apercevrez assez rapidement que ce qui est au moins aussi important que les ensembles, ce sont les relations entre ensembles : ce sera la notion d'application (ou fonction) entre deux ensembles.

1. Ensembles

1.1. Définir des ensembles

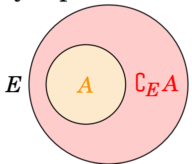
- On va définir informellement ce qu'est un ensemble : un ***ensemble*** est une collection d'éléments.
- Exemples :
$$\{0,1\}, \quad \{\text{rouge}, \text{noir}\}, \quad \{0,1,2,3,\dots\} = \mathbb{N}.$$
- Un ensemble particulier est l'***ensemble vide***, noté $\varnothing$ qui est l'ensemble ne contenant aucun élément.
- On note
$$\boxed{x \in E}$$
si x est un élément de E, et $x \notin E$ dans le cas contraire.
- Voici une autre façon de définir des ensembles : une collection d'éléments qui vérifient une propriété.
- Exemples :
$$\left\{x \in \mathbb{R} \mid |x-2| < 1\right\}, \quad \left\{z \in \mathbb{C} \mid z^5 = 1\right\}, \quad \left\{x \in \mathbb{R} \mid 0 \leqslant x \leqslant 1\right\} = [0,1].$$

1.2. Inclusion, union, intersection, complémentaire

- L'***inclusion***. $E \subset F$ si tout élément de E est aussi un élément de F (autrement dit : $\forall x \in E\ (x \in F)$). On dit alors que E est un ***sous-ensemble*** de F ou une ***partie*** de F.
- L'***égalité***. $E = F$ si et seulement si $E \subset F$ et $F \subset E$.
- ***Ensemble des parties*** de E. On note $\mathscr{P}(E)$ l'ensemble des parties de E. Par exemple si $E = \{1,2,3\}$:
$$\mathscr{P}(\{1,2,3\}) = \left\{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\right\}.$$
- ***Complémentaire***. Si $A \subset E$,

$$\complement_E A = \{x \in E \mid x \notin A\}$$

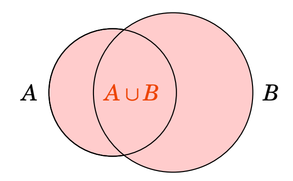
On le note aussi $E \setminus A$ et juste $\complement A$ s'il n'y a pas d'ambiguïté (et parfois aussi A^c ou $\overline{A}$).



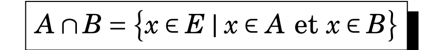
– ***Union***. Pour $A, B \subset E$,

$$A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$$

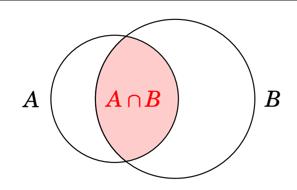
Le *«ou»* n'est pas exclusif : x peut appartenir à A et à B en même temps.



– ***Intersection***.



$$A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$$



1.3. Règles de calculs

Soient A, B, C des parties d'un ensemble E.

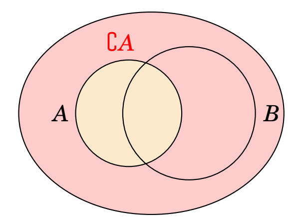
– $A \cap B = B \cap A$
– $A \cap (B \cap C) = (A \cap B) \cap C$ (on peut donc écrire $A \cap B \cap C$ sans ambigüité)
– $A \cap \varnothing = \varnothing, \quad A \cap A = A, \quad A \subset B \iff A \cap B = A$

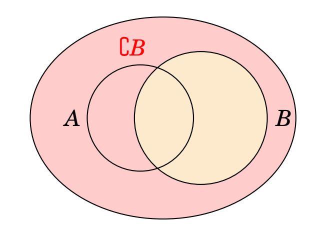
– $A \cup B = B \cup A$
– $A \cup (B \cup C) = (A \cup B) \cup C$ (on peut donc écrire $A \cup B \cup C$ sans ambigüité)
– $A \cup \varnothing = A, \quad A \cup A = A, \quad A \subset B \iff A \cup B = B$

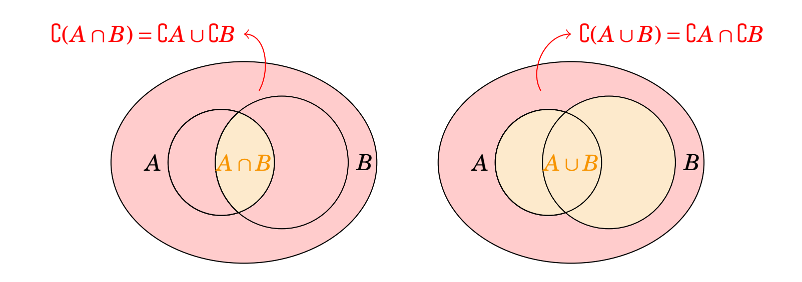
– $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
– $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

– $\complement\left(\complement A\right) = A$ et donc $A \subset B \iff \complement B \subset \complement A$.
– $\complement(A \cap B) = \complement A \cup \complement B$
– $\complement(A \cup B) = \complement A \cap \complement B$

Voici les dessins pour les deux dernières assertions.







Les preuves sont pour l'essentiel une reformulation des opérateurs logiques, en voici quelques-unes :

- Preuve de $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$: $x\in A\cap(B\cup C) \iff x\in A$ et $x\in(B\cup C) \iff x\in A$ et ($x\in B$ ou $x\in C$) $\iff$ ($x\in A$ et $x\in B$) ou ($x\in A$ et $x\in C$) $\iff (x\in A\cap B)$ ou $(x\in A\cap C) \iff x\in(A\cap B)\cup(A\cap C)$.
- Preuve de $\complement(A\cap B)=\complement A\cup\complement B$: $x\in\complement(A\cap B) \iff x\notin(A\cap B) \iff \text{non}\big(x\in A\cap B\big) \iff \text{non}\big(x\in A \text{ et } x\in B\big) \iff \text{non}(x\in A)$ ou $\text{non}(x\in B) \iff x\notin A$ ou $x\notin B \iff x\in\complement A\cup\complement B$.

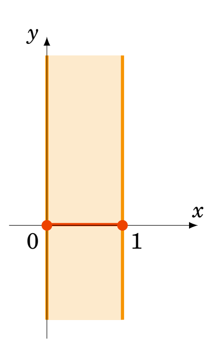
Remarquez que l'on repasse aux éléments pour les preuves.

1.4. Produit cartésien

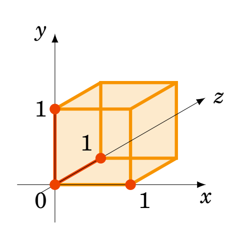
Soient E et F deux ensembles. Le ***produit cartésien***, noté $E\times F$, est l'ensemble des couples (x,y) où $x\in E$ et $y\in F$.

Exemple 7

1. Vous connaissez $\mathbb{R}^2=\mathbb{R}\times\mathbb{R}=\big\{(x,y)\mid x,y\in\mathbb{R}\big\}$.
2. Autre exemple $[0,1]\times\mathbb{R}=\big\{(x,y)\mid 0\leqslant x\leqslant 1, y\in\mathbb{R}\big\}$



3. $[0,1]\times[0,1]\times[0,1]=\big\{(x,y,z)\mid 0\leqslant x,y,z\leqslant 1\big\}$



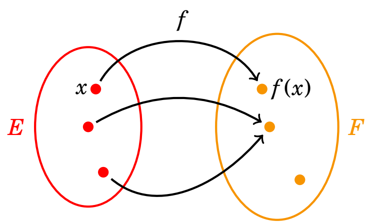
Mini-exercices

1. En utilisant les définitions, montrer : $A \neq B$ si et seulement s'il existe $a \in A \setminus B$ ou $b \in B \setminus A$.
2. Énumérer $\mathscr{P}(\{1,2,3,4\})$.
3. Montrer $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ et $\complement(A \cup B) = \complement A \cap \complement B$.
4. Énumérer $\{1,2,3\} \times \{1,2,3,4\}$.
5. Représenter les sous-ensembles de $\mathbb{R}^2$ suivants : $\big(]0,1[\cup[2,3[\big) \times [-1,1]$, $\big(\mathbb{R} \setminus (]0,1[\cup[2,3[\big) \times \big((\mathbb{R} \setminus [-1,1]) \cap [0,2]\big)$.

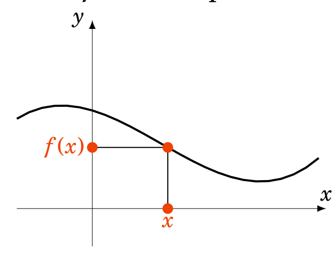
2. Applications

2.1. Définitions

- Une ***application*** (ou une ***fonction***) $f : E \to F$, c'est la donnée pour chaque élément $x \in E$ d'un unique élément de F noté $f(x)$.
  Nous représenterons les applications par deux types d'illustrations : les ensembles «patates», l'ensemble de départ (et celui d'arrivée) est schématisé par un ovale ses éléments par des points. L'association $x \mapsto f(x)$ est représentée par une flèche.



  L'autre représentation est celle des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ (ou des sous-ensembles de $\mathbb{R}$). L'ensemble de départ $\mathbb{R}$ est représenté par l'axe des abscisses et celui d'arrivée par l'axe des ordonnées. L'association $x \mapsto f(x)$ est représentée par le point $(x, f(x))$.



- ***Égalité***. Deux applications $f, g : E \to F$ sont égales si et seulement si pour tout $x \in E$, $f(x) = g(x)$. On note alors $f = g$.
- Le ***graphe*** de $f : E \to F$ est

$$\Gamma_f = \Big\{\big(x, f(x)\big) \in E \times F \mid x \in E\Big\}$$

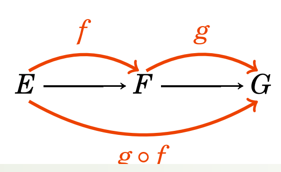
y

Γ_f

x

- ***Composition***. Soient $f : E \to F$ et $g : F \to G$ alors $g \circ f : E \to G$ est l'application définie par

$$g \circ f(x) = g\big(f(x)\big).$$



Exemple 8

1. L'***identité***, $\mathrm{id}_E : E \to E$ est simplement définie par $x \mapsto x$ et sera très utile dans la suite.
2. Définissons f, g ainsi

$$f : \begin{array}{ccc}]0,+\infty[& \longrightarrow &]0,+\infty[\\ x & \longmapsto & \frac{1}{x} \end{array}, \qquad g : \begin{array}{ccc}]0,+\infty[& \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{x-1}{x+1} \end{array}.$$

Alors $g \circ f :]0,+\infty[\to \mathbb{R}$ vérifie pour tout $x \in]0,+\infty[$:

$$g \circ f(x) = g\big(f(x)\big) = g\left(\frac{1}{x}\right) = \frac{\frac{1}{x} - 1}{\frac{1}{x} + 1} = \frac{1-x}{1+x} = -g(x).$$

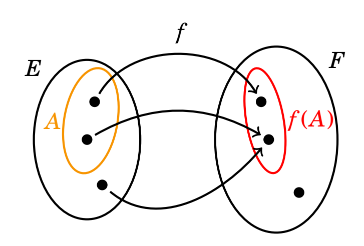
2.2. Image directe, image réciproque

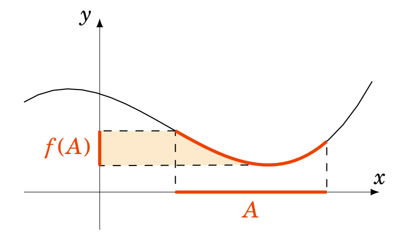
Soient E, F deux ensembles.

Définition 1

Soit $A \subset E$ et $f : E \to F$, l'***image directe*** de A par f est l'ensemble

$$f(A) = \big\{ f(x) \mid x \in A \big\}$$

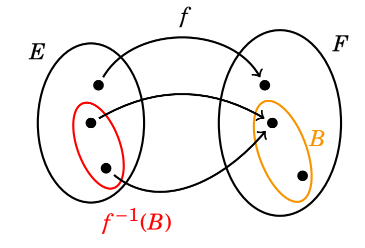


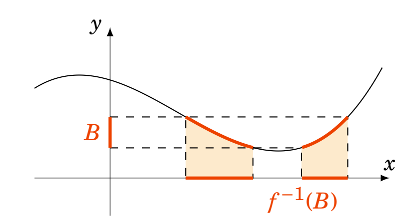


Définition 2

Soit $B \subset F$ et $f : E \to F$, l'***image réciproque*** de B par f est l'ensemble

$$f^{-1}(B) = \big\{ x \in E \mid f(x) \in B \big\}$$





Remarque

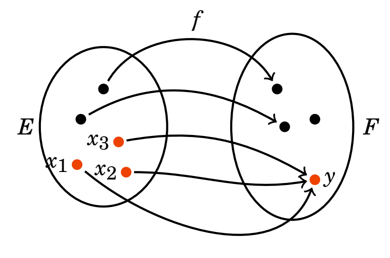
Ces notions sont plus difficiles à maîtriser qu'il n'y paraît !

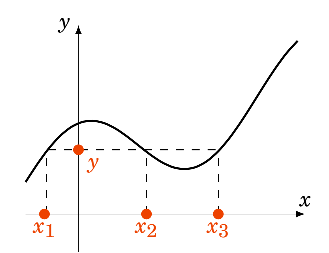
- $f(A)$ est un sous-ensemble de F, $f^{-1}(B)$ est un sous-ensemble de E.
- La notation «$f^{-1}(B)$» est un tout, rien ne dit que f est un fonction bijective (voir plus loin). L'image réciproque existe quelque soit la fonction.
- L'image directe d'un singleton $f(\{x\}) = \{f(x)\}$ est un singleton. Par contre l'image réciproque d'un singleton $f^{-1}(\{y\})$ dépend de f. Cela peut être un singleton, un ensemble à plusieurs éléments ; mais cela peut-être E tout entier (si f est une fonction constante) ou même l'ensemble vide (si aucune image par f ne vaut y).

2.3. Antécédents

Fixons $y \in F$. Tout élément $x \in E$ tel que $f(x) = y$ est un ***antécédent*** de y.
En termes d'image réciproque l'ensemble des antécédents de y est $f^{-1}(\{y\})$.

Sur les dessins suivants, l'élément y admet 3 antécédents par f. Ce sont x_1, x_2, x_3.





Mini-exercices

1. Pour deux applications $f, g : E \to F$, quelle est la négation de $f = g$?
2. Représenter le graphe de $f : \mathbb{N} \to \mathbb{R}$ définie par $n \mapsto \frac{4}{n+1}$.
3. Soient $f, g, h : \mathbb{R} \to \mathbb{R}$ définies par $f(x) = x^2$, $g(x) = 2x+1$, $h(x) = x^3 - 1$. Calculer $f \circ (g \circ h)$ et $(f \circ g) \circ h$.
4. Pour la fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $x \mapsto x^2$ représenter et calculer les ensembles suivants : $f([0,1[)$, $f(\mathbb{R})$, $f(]-1,2[)$, $f^{-1}([1,2[)$, $f^{-1}([-1,1])$, $f^{-1}(\{3\})$, $f^{-1}(\mathbb{R} \setminus \mathbb{N})$.

3. Injection, surjection, bijection

3.1. Injection, surjection

Soit E, F deux ensembles et $f : E \to F$ une application.

Définition 3

f est ***injective*** si pour tout $x, x' \in E$ avec $f(x) = f(x')$ alors $x = x'$. Autrement dit :

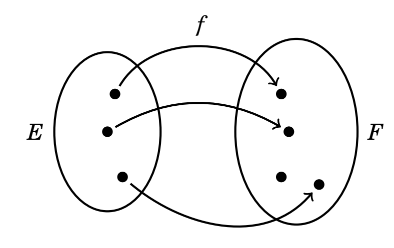
$$\forall x, x' \in E \quad \big(f(x) = f(x') \implies x = x'\big)$$

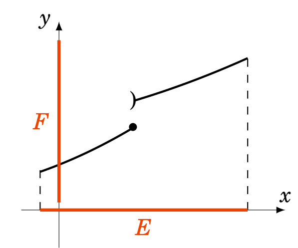
Définition 4

f est ***surjective*** si pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$. Autrement dit :

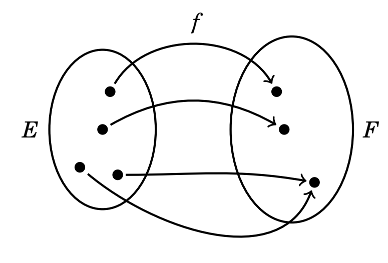
$$\forall y \in F \quad \exists x \in E \quad \big(y = f(x)\big)$$

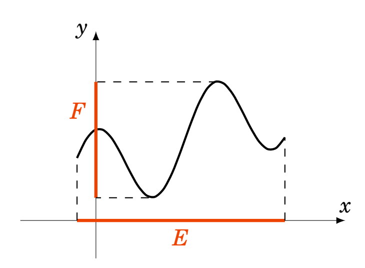
Une autre formulation : f est surjective si et seulement si $f(E) = F$.
Les applications f représentées sont injectives :





Les applications f représentées sont surjectives :





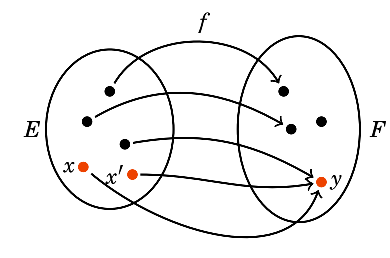
Remarque

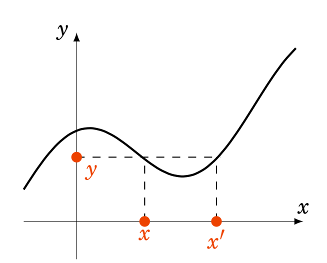
Encore une fois ce sont des notions difficiles à appréhender. Une autre façon de formuler l'injectivité et la surjectivité est d'utiliser les antécédents.

- f est injective si et seulement si tout élément y de F a *au plus* 1 antécédent (et éventuellement aucun).
- f est surjective si et seulement si tout élément y de F a *au moins* 1 antécédent.

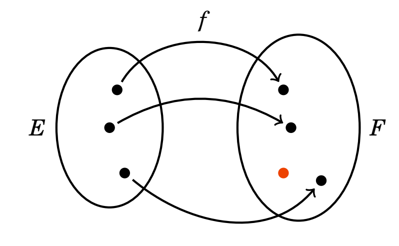
Remarque

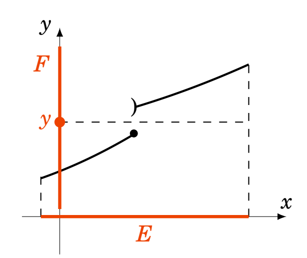
Voici deux fonctions non injectives :





Ainsi que deux fonctions non surjectives :





Exemple 9

1. Soit $f_1 : \mathbb{N} \to \mathbb{Q}$ définie par $f_1(x) = \frac{1}{1+x}$. Montrons que f_1 est injective : soit $x, x' \in \mathbb{N}$ tels que $f_1(x) = f_1(x')$. Alors $\frac{1}{1+x} = \frac{1}{1+x'}$, donc $1+x = 1+x'$ et donc $x = x'$. Ainsi f_1 est injective.
   Par contre f_1 n'est pas surjective. Il s'agit de trouver un élément y qui n'a pas d'antécédent par f_1. Ici il est facile de voir que l'on a toujours $f_1(x) \leqslant 1$ et donc par exemple $y = 2$ n'a pas d'antécédent. Ainsi f_1 n'est pas surjective.
2. Soit $f_2 : \mathbb{Z} \to \mathbb{N}$ définie par $f_2(x) = x^2$. Alors f_2 n'est pas injective. En effet on peut trouver deux éléments $x, x' \in \mathbb{Z}$ différents tels que $f_2(x) = f_2(x')$. Il suffit de prendre par exemple $x = 2$, $x' = -2$.

   f_2 n'est pas non plus surjective, en effet il existe des éléments $y \in \mathbb{N}$ qui n'ont aucun antécédent. Par exemple $y = 3$: si $y = 3$ avait un antécédent x par f_2, nous aurions $f_2(x) = y$, c'est-à-dire $x^2 = 3$, d'où $x = \pm\sqrt{3}$. Mais alors x n'est pas un entier de $\mathbb{Z}$. Donc $y = 3$ n'a pas d'antécédent et f_2 n'est pas surjective.

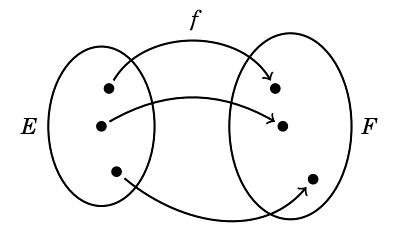
3.2. Bijection

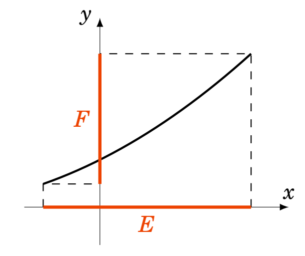
Définition 5

f est ***bijective*** si elle injective et surjective. Cela équivaut à : pour tout $y \in F$ il existe un unique $x \in E$ tel que $y = f(x)$. Autrement dit :

$$\forall y \in F \quad \exists! x \in E \quad \big(y = f(x)\big)$$

L'existence du x vient de la surjectivité et l'unicité de l'injectivité. Autrement dit, tout élément de F a un unique antécédent par f.





Proposition 2

Soit E, F des ensembles et $f : E \to F$ une application.

1. L'application f est bijective si et seulement si il existe une application $g : F \to E$ telle que $f \circ g = \mathrm{id}_F$ et $g \circ f = \mathrm{id}_E$.
2. Si f est bijective alors l'application g est unique et elle aussi est bijective. L'application g s'appelle la ***bijection réciproque*** de f et est notée f^{-1}. De plus $\left(f^{-1}\right)^{-1} = f$.

Remarque

- $f \circ g = \mathrm{id}_F$ se reformule ainsi

$$\forall y \in F \quad f\big(g(y)\big) = y.$$

- Alors que $g \circ f = \mathrm{id}_E$ s'écrit :

$$\forall x \in E \quad g\big(f(x)\big) = x.$$

- Par exemple $f : \mathbb{R} \to]0, +\infty[$ définie par $f(x) = \exp(x)$ est bijective, sa bijection réciproque est $g :]0, +\infty[\to \mathbb{R}$ définie par $g(y) = \ln(y)$. Nous avons bien $\exp\big(\ln(y)\big) = y$, pour tout $y \in]0, +\infty[$ et $\ln\big(\exp(x)\big) = x$, pour tout $x \in \mathbb{R}$.

Démonstration

1. – Sens $\Rightarrow$. Supposons f bijective. Nous allons construire une application $g : F \to E$. Comme f est surjective alors pour chaque $y \in F$, il existe un $x \in E$ tel que $y = f(x)$ et on pose $g(y) = x$. On a $f\big(g(y)\big) = f(x) = y$, ceci pour tout $y \in F$ et donc $f \circ g = \mathrm{id}_F$. On compose à droite avec f donc $f \circ g \circ f = \mathrm{id}_F \circ f$. Alors pour tout $x \in E$ on a $f\big(g \circ f(x)\big) = f(x)$ or f est injective et donc $g \circ f(x) = x$. Ainsi $g \circ f = \mathrm{id}_E$. Bilan : $f \circ g = \mathrm{id}_F$ et $g \circ f = \mathrm{id}_E$.
   – Sens $\Leftarrow$. Supposons que g existe et montrons que f est bijective.
     – f est surjective : en effet soit $y \in F$ alors on note $x = g(y) \in E$; on a bien : $f(x) = f\big(g(y)\big) = f \circ g(y) = \mathrm{id}_F(y) = y$, donc f est bien surjective.
     – f est injective : soient $x, x' \in E$ tels que $f(x) = f(x')$. On compose par g (à gauche) alors $g \circ f(x) = g \circ f(x')$ donc $\mathrm{id}_E(x) = \mathrm{id}_E(x')$ donc $x = x'$; f est bien injective.
2. – Si f est bijective alors g est aussi bijective car $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$ et on applique ce que l'on vient de démontrer avec g à la place de f. Ainsi $g^{-1} = f$.
   – Si f est bijective, g est unique : en effet soit $h : F \to E$ une autre application telle que $h \circ f = \mathrm{id}_E$ et $f \circ h = \mathrm{id}_F$; en particulier $f \circ h = \mathrm{id}_F = f \circ g$, donc pour tout $y \in F$, $f\big(h(y)\big) = f\big(g(y)\big)$ or f est injective alors $h(y) = g(y)$, ceci pour tout $y \in F$; d'où $h = g$.

Proposition 3

Soient $f : E \to F$ et $g : F \to G$ des applications bijectives. L'application $g \circ f$ est bijective et sa bijection réciproque est

$$\boxed{(g \circ f)^{-1} = f^{-1} \circ g^{-1}}$$

Démonstration

D'après la proposition 2, il existe $u : F \to E$ tel que $u \circ f = \mathrm{id}_E$ et $f \circ u = \mathrm{id}_F$. Il existe aussi $v : G \to F$ tel que $v \circ g = \mathrm{id}_F$ et $g \circ v = \mathrm{id}_G$. On a alors $(g \circ f) \circ (u \circ v) = g \circ (f \circ u) \circ v = g \circ \mathrm{id}_F \circ u = g \circ u = \mathrm{id}_E$. Et $(u \circ v) \circ (g \circ f) = u \circ (v \circ g) \circ f = u \circ \mathrm{id}_F \circ f = u \circ f = \mathrm{id}_E$. Donc $g \circ f$ est bijective et son inverse est $u \circ v$. Comme u est la bijection réciproque de f et v celle de g alors : $u \circ v = f^{-1} \circ g^{-1}$.

Mini-exercices

1. Les fonctions suivantes sont-elles injectives, surjectives, bijectives ?
   - $f_1 : \mathbb{R} \to [0, +\infty[$, $x \mapsto x^2$.
   - $f_2 : [0, +\infty[\to [0, +\infty[$, $x \mapsto x^2$.
   - $f_3 : \mathbb{N} \to \mathbb{N}$, $x \mapsto x^2$.
   - $f_4 : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x - 7$.
   - $f_5 : \mathbb{R} \to [0, +\infty[$, $x \mapsto |x|$.
2. Montrer que la fonction $f :]1, +\infty[\to]0, +\infty[$ définie par $f(x) = \frac{1}{x-1}$ est bijective. Calculer sa bijection réciproque.

4. Ensembles finis

4.1. Cardinal

Définition 6

Un ensemble E est ***fini*** s'il existe un entier $n \in \mathbb{N}$ et une bijection de E vers $\{1, 2, \ldots, n\}$. Cet entier n est unique et s'appelle le ***cardinal*** de E (ou le ***nombre d'éléments***) et est noté $\operatorname{Card} E$.

Quelques exemples :

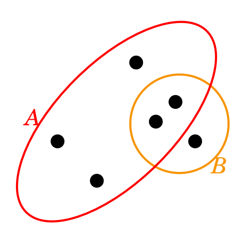
1. $E = \{\text{rouge}, \text{noir}\}$ est en bijection avec $\{1, 2\}$ et donc est de cardinal 2.
2. $\mathbb{N}$ n'est pas un ensemble fini.
3. Par définition le cardinal de l'ensemble vide est 0.

Enfin quelques propriétés :

1. Si A est un ensemble fini et $B \subset A$ alors B est un ensemble fini et $\operatorname{Card} B \leqslant \operatorname{Card} A$.
2. Si A, B sont des ensembles finis disjoints (c'est-à-dire $A \cap B = \varnothing$) alors $\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B$.
3. Si A est un ensemble fini et $B \subset A$ alors $\operatorname{Card}(A \setminus B) = \operatorname{Card} A - \operatorname{Card} B$.
4. Enfin pour A, B deux ensembles finis quelconques :

$$\boxed{\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B - \operatorname{Card}(A \cap B)}$$

Voici une situation où s'applique la dernière propriété :



4.2. Injection, surjection, bijection et ensembles finis

Proposition 4

Soit E, F deux ensembles finis et $f : E \to F$ une application.

1. Si f est injective alors $\operatorname{Card} E \leqslant \operatorname{Card} F$.
2. Si f est surjective alors $\operatorname{Card} E \geqslant \operatorname{Card} F$.
3. Si f est bijective alors $\operatorname{Card} E = \operatorname{Card} F$.

Démonstration

1. Supposons f injective. Notons $F' = f(E) \subset F$ alors la restriction $f_| : E \to F'$ (définie par $f_|(x) = f(x)$) est une bijection. Donc pour chaque $y \in F'$ est associé un unique $x \in E$ tel que $y = f(x)$. Donc E et F' ont le même nombre d'éléments. Donc $\operatorname{Card} F' = \operatorname{Card} E$. Or $F' \subset F$, ainsi $\operatorname{Card} E = \operatorname{Card} F' \leqslant \operatorname{Card} F$.
2. Supposons f surjective. Pour tout élément $y \in F$, il existe au moins un élément x de E tel que $y = f(x)$ et donc $\operatorname{Card} E \geqslant \operatorname{Card} F$.
3. Cela découle de (1) et (2) (ou aussi de la preuve du (1)).

Proposition 5

Soit E, F deux ensembles finis et $f : E \to F$ une application. Si

$$\operatorname{Card} E = \operatorname{Card} F$$

alors les assertions suivantes sont équivalentes :

i. f est injective,
ii. f est surjective,
iii. f est bijective.

Démonstration

Le schéma de la preuve est le suivant : nous allons montrer successivement les implications :

$$(i) \implies (ii) \implies (iii) \implies (i)$$

ce qui prouvera bien toutes les équivalences.

– $(i) \implies (ii)$. Supposons f injective. Alors $\operatorname{Card} f(E) = \operatorname{Card} E = \operatorname{Card} F$. Ainsi $f(E)$ est un

sous-ensemble de F ayant le même cardinal que F ; cela entraîne $f(E) = F$ et donc f est surjective.

- $(ii) \implies (iii)$. Supposons f surjective. Pour montrer que f est bijective, il reste à montrer que f est injective. Raisonnons par l'absurde et supposons f non injective. Alors $\operatorname{Card} f(E) < \operatorname{Card} E$ (car au moins 2 éléments ont la même image). Or $f(E) = F$ car f surjective, donc $\operatorname{Card} F < \operatorname{Card} E$. C'est une contradiction, donc f doit être injective et ainsi f est bijective.
- $(iii) \implies (i)$. C'est clair : une fonction bijective est en particulier injective.

Appliquez ceci pour montrer le ***principe des tiroirs*** :

Proposition 6

Si l'on range dans k tiroirs, $n > k$ paires de chaussettes alors il existe (au moins) un tiroir contenant (au moins) deux paires de chaussettes.

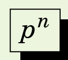
Malgré sa formulation amusante, c'est une proposition souvent utile. Exemple : dans un amphi de 400 étudiants, il y a au moins deux étudiants nés le même jour !

4.3. Nombres d'applications

Soient E, F des ensembles finis, non vides. On note $\operatorname{Card} E = n$ et $\operatorname{Card} F = p$.

Proposition 7

Le nombre d'applications différentes de E dans F est :



$$p^n$$

Autrement dit c'est $(\operatorname{Card} F)^{\operatorname{Card} E}$.

Exemple 10

En particulier le nombre d'applications de E dans lui-même est n^n. Par exemple si $E = \{1, 2, 3, 4, 5\}$ alors ce nombre est $5^5 = 3125$.

Démonstration

Fixons F et $p = \operatorname{Card} F$. Nous allons effectuer une récurrence sur $n = \operatorname{Card} E$. Soit (P_n) l'assertion suivante : le nombre d'applications d'un ensemble à n éléments vers un ensemble à p éléments est p^n.

- *Initialisation.* Pour $n = 1$, une application de E dans F est définie par l'image de l'unique élément de E. Il y a $p = \operatorname{Card} F$ choix possibles et donc p^1 applications distinctes. Ainsi P_1 est vraie.
- *Hérédité.* Fixons $n \geqslant 1$ et supposons que P_n est vraie. Soit E un ensemble à $n+1$ éléments. On choisit et fixe $a \in E$; soit alors $E' = E \setminus \{a\}$ qui a bien n éléments. Le nombre d'applications de E' vers F est p^n, par l'hypothèse de récurrence (P_n). Pour chaque application $f : E' \to F$ on peut la prolonger en une application $f : E \to F$ en choisissant l'image de a. On a p choix pour l'image de a et donc $p^n \times p$ choix pour les applications de E vers F. Ainsi P_{n+1} est vérifiée.
- *Conclusion.* Par le principe de récurrence P_n est vraie, pour tout $n \geqslant 1$.

Proposition 8

Le nombre d'injections de E dans F est :

$$p \times (p-1) \times \cdots \times (p-(n-1)).$$

Démonstration

Supposons $E = \{a_1, a_2, \ldots, a_n\}$; pour l'image de a_1 nous avons p choix. Une fois ce choix fait, pour l'image de a_2 il reste $p-1$ choix (car a_2 ne doit pas avoir la même image que a_1). Pour l'image de a_3 il y a $p-2$ possibilités. Ainsi de suite : pour l'image de a_k il y $p-(k-1)$ choix... Il y a au final $p \times (p-1) \times \cdots \times (p-(n-1))$ applications injectives.

Notation ***factorielle*** : $n! = 1 \times 2 \times 3 \times \cdots \times n$. Avec $1! = 1$ et par convention $0! = 1$.

Proposition 9

Le nombre de bijections d'un ensemble E de cardinal n dans lui-même est :



Exemple 11

Parmi les 3125 applications de $\{1,2,3,4,5\}$ dans lui-même il y en a $5! = 120$ qui sont bijectives.

Démonstration

Nous allons le prouver par récurrence sur n. Soit (P_n) l'assertion suivante : le nombre de bijections d'un ensemble à n éléments dans un ensemble à n éléments est $n!$

- P_1 est vraie. Il n'y a qu'une bijection d'un ensemble à 1 élément dans un ensemble à 1 élément.
- Fixons $n \geqslant 1$ et supposons que P_n est vraie. Soit E un ensemble à $n+1$ éléments. On fixe $a \in E$. Pour chaque $b \in E$ il y a -par l'hypothèse de récurrence- exactement $n!$ applications bijectives de $E \setminus \{a\} \to E \setminus \{b\}$. Chaque application se prolonge en une bijection de $E \to F$ en posant $a \mapsto b$. Comme il y a $n+1$ choix de $b \in E$ alors nous obtenons $n! \times (n+1)$ bijections de E dans lui-même. Ainsi P_{n+1} est vraie.
- Par le principe de récurrence le nombre de bijections d'un ensemble à n éléments est $n!$

On aurait aussi pu directement utiliser la proposition 8 avec $n = p$ (sachant qu'alors les injections sont aussi des bijections).

4.4. Nombres de sous-ensembles

Soit E un ensemble fini de cardinal n.

Proposition 10

Il y a $2^{\operatorname{Card} E}$ sous-ensembles de E :

$$\boxed{\operatorname{Card}\mathscr{P}(E) = 2^n}$$

Exemple 12

Si $E = \{1,2,3,4,5\}$ alors $\mathscr{P}(E)$ a $2^5 = 32$ parties. C'est un bon exercice de les énumérer :
- l'ensemble vide : $\varnothing$,
- 5 singletons : $\{1\},\{2\},\ldots$,
- 10 paires : $\{1,2\},\{1,3\},\ldots,\{2,3\},\ldots$,
- 10 triplets : $\{1,2,3\},\ldots$,
- 5 ensembles à 4 éléments : $\{1,2,3,4\},\{1,2,3,5\},\ldots$,
- et E tout entier : $\{1,2,3,4,5\}$.

Démonstration

Encore une récurrence sur $n = \operatorname{Card} E$.
- Si $n = 1$, $E = \{a\}$ est un singleton, les deux sous-ensembles sont : $\varnothing$ et E.
- Supposons que la proposition soit vraie pour $n \geqslant 1$ fixé. Soit E un ensemble à $n+1$ éléments. On fixe $a \in E$. Il y a deux sortes de sous-ensembles de E :
  - les sous-ensembles A qui ne contiennent pas a : ce sont les sous-ensembles $A \subset E \setminus \{a\}$. Par l'hypothèse de récurrence il y en a 2^n.
  - les sous-ensembles A qui contiennent a : ils sont de la forme $A = \{a\} \cup A'$ avec $A' \subset E \setminus \{a\}$. Par l'hypothèse de récurrence il y a 2^n sous-ensembles A' possibles et donc aussi 2^n sous-ensembles A.

  Le bilan : $2^n + 2^n = 2^{n+1}$ parties $A \subset E$.
- Par le principe de récurrence, nous avons prouvé que si $\operatorname{Card} E = n$ alors $\operatorname{Card}\mathscr{P}(E) = 2^n$.

4.5. Coefficients du binôme de Newton

Définition 7

Le nombre de parties à k éléments d'un ensemble à n éléments est noté $\binom{n}{k}$ ou C_n^k.

Exemple 13

Les parties à deux éléments de $\{1,2,3\}$ sont $\{1,2\}$, $\{1,3\}$ et $\{2,3\}$ et donc $\binom{3}{2} = 3$. Nous avons déjà classé les parties de $\{1,2,3,4,5\}$ par nombre d'éléments et donc
- $\binom{5}{0} = 1$ (la seule partie n'ayant aucun élément est l'ensemble vide),
- $\binom{5}{1} = 5$ (il y a 5 singletons),
- $\binom{5}{2} = 10$ (il y a 10 paires),
- $\binom{5}{3} = 10$,
- $\binom{5}{4} = 5$,
- $\binom{5}{5} = 1$ (la seule partie ayant 5 éléments est l'ensemble tout entier).

Sans calculs on peut déjà remarquer les faits suivants :

Proposition 11

- $\binom{n}{0} = 1$, $\binom{n}{1} = n$, $\binom{n}{n} = 1$.
- $\boxed{\binom{n}{n-k} = \binom{n}{k}}$
- $\boxed{\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n} = 2^n}$

Démonstration

1. Par exemple : $\binom{n}{1} = n$ car il y a n singletons.
2. Compter le nombre de parties $A \subset E$ ayant k éléments revient aussi à compter le nombre de parties de la forme $\complement A$ (qui ont donc $n-k$ éléments), ainsi $\binom{n}{n-k} = \binom{n}{k}$.
3. La formule $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n} = 2^n$ exprime que faire la somme du nombre de parties à k éléments, pour $k = 0, \ldots, n$, revient à compter toutes les parties de E.

Proposition 12

$$\boxed{\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \qquad 0 < k < n}$$

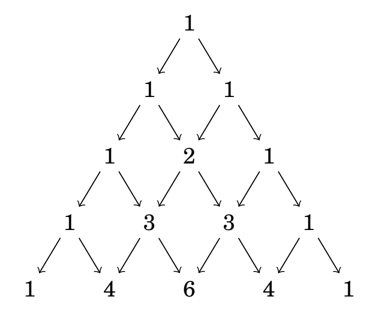
Démonstration

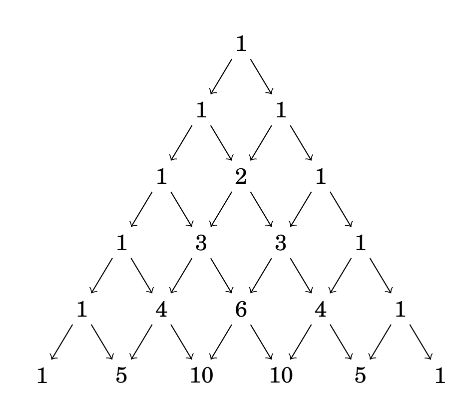
Soit E un ensemble à n éléments, $a \in E$ et $E' = E \setminus \{a\}$. Il y a deux sortes de parties $A \subset E$ ayant k éléments :

- celles qui ne contiennent pas a : ce sont donc des parties à k éléments dans E' qui a $n-1$ éléments. Il y a en a donc $\binom{n-1}{k}$,
- celles qui contiennent a : elles sont de la forme $A = \{a\} \cup A'$ avec A' une partie à $k-1$ éléments dans E' qui a $n-1$ éléments. Il y en a $\binom{n-1}{k-1}$.

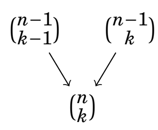
Bilan : $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Le triangle de Pascal est un algorithme pour calculer ces coefficients $\binom{n}{k}$. La ligne du haut correspond à $\binom{0}{0}$, la ligne suivante à $\binom{1}{0}$ et $\binom{1}{1}$, la ligne d'après à $\binom{2}{0}$, $\binom{2}{1}$ et $\binom{2}{2}$.
La dernière ligne du triangle de gauche aux coefficients $\binom{4}{0}$, $\binom{4}{1}$, ..., $\binom{4}{4}$.
Comment continuer ce triangle pour obtenir le triangle de droite ? Chaque élément de la nouvelle ligne est obtenu en ajoutant les deux nombres qui lui sont au-dessus à droite et au-dessus à gauche.





Ce qui fait que cela fonctionne c'est bien sûr la proposition 12 qui se représente ainsi :



Une autre façon de calculer le coefficient du binôme de Newton repose sur la formule suivante :

Proposition 13

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Démonstration

Cela se fait par récurrence sur n. C'est clair pour $n = 1$. Si c'est vrai au rang $n-1$ alors écrivons $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ et utilisons l'hypothèse de récurrence pour $\binom{n-1}{k-1}$ et $\binom{n-1}{k}$. Ainsi

$$\begin{aligned}\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!} \\ &= \frac{(n-1)!}{(k-1)!(n-k-1)!} \times \left(\frac{1}{n-k} + \frac{1}{k}\right) = \frac{(n-1)!}{(k-1)!(n-k-1)!} \times \frac{n}{k(n-k)} \\ &= \frac{n!}{k!(n-k)!}\end{aligned}$$

4.6. Formule du binôme de Newton

Théorème 1

Soient $a, b \in \mathbb{R}$ et n un entier positif alors :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k$$

Autrement dit :

$$(a+b)^n = \binom{n}{0} a^n \cdot b^0 + \binom{n}{1} a^{n-1} \cdot b^1 + \cdots + \binom{n}{k} a^{n-k} \cdot b^k + \cdots + \binom{n}{n} a^0 \cdot b^n$$

Le théorème est aussi vrai si a et b sont des nombres complexes.

Exemple 14

1. Pour $n = 2$ on retrouve la formule archi-connue : $(a+b)^2 = a^2 + 2ab + b^2$.
2. Il est aussi bon de connaître $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.
3. Si $a = 1$ et $b = 1$ on retrouve la formule : $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Démonstration

Nous allons effectuer une récurrence sur n. Soit (P_n) l'assertion : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k$.

- *Initialisation.* Pour $n = 1$, $(a+b)^1 = \binom{1}{0}a^1b^0 + \binom{1}{1}a^0b^1$. Ainsi P_1 est vraie.
- *Hérédité.* Fixons $n \geqslant 2$ et supposons que P_{n-1} est vraie.

$$\begin{aligned}
(a+b)^n = (a+b)\cdot(a+b)^{n-1} &= a\left(a^{n-1}+\cdots+\binom{n-1}{k}a^{n-1-k}b^k+\cdots+b^{n-1}\right)\\
&\quad +b\left(a^{n-1}+\cdots+\binom{n-1}{k-1}a^{n-1-(k-1)}b^{k-1}+\cdots+b^{n-1}\right)\\
&= \cdots+\left(\binom{n-1}{k}+\binom{n-1}{k-1}\right)a^{n-k}b^k+\cdots\\
&= \cdots+\binom{n}{k}a^{n-k}b^k+\cdots = \sum_{k=0}^{n}\binom{n}{k}\,a^{n-k}\cdot b^k
\end{aligned}$$

  Ainsi P_{n+1} est vérifiée.
- *Conclusion.* Par le principe de récurrence P_n est vraie, pour tout $n \geqslant 1$.

Mini-exercices

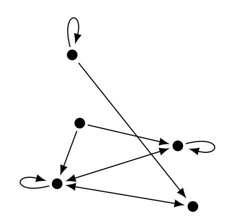
1. Combien y a-t-il d'applications injectives d'un ensemble à n éléments dans un ensemble à $n+1$ éléments ?
2. Combien y a-t-il d'applications surjectives d'un ensemble à $n+1$ éléments dans un ensemble à n éléments ?
3. Calculer le nombre de façons de choisir 5 cartes dans un jeux de 32 cartes.
4. Calculer le nombre de listes à k éléments dans un ensemble à n éléments (les listes sont ordonnées : par exemple $(1,2,3) \neq (1,3,2)$).
5. Développer $(a-b)^4$, $(a+b)^5$.
6. Que donne la formule du binôme pour $a = -1$, $b = +1$? En déduire que dans un ensemble à n éléments il y a autant de parties de cardinal pair que de cardinal impair.

5. Relation d'équivalence

5.1. Définition

Une ***relation*** sur un ensemble E, c'est la donnée pour tout couple $(x,y) \in E \times E$ de «Vrai» (s'ils sont en relation), ou de «Faux» sinon.

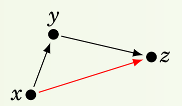
Nous schématisons une relation ainsi : les éléments de E sont des points, une flèche de x vers y signifie que x est en relation avec y, c'est-à-dire que l'on associe «Vrai» au couple (x,y).



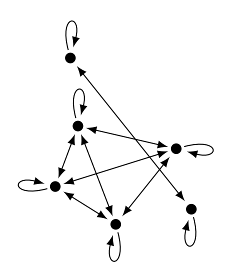
Définition 8

Soit E un ensemble et $\mathscr{R}$ une relation, c'est une ***relation d'équivalence*** si :

- $\forall x \in E,\ x\mathscr{R}x,$ (***réflexivité***)
- $\forall x, y \in E,\ x\mathscr{R}y \implies y\mathscr{R}x,$ (***symétrie***)
- $\forall x, y, z \in E,\ x\mathscr{R}y$ et $y\mathscr{R}z \implies x\mathscr{R}z,$ (***transitivité***)



Exemple de relation d'équivalence :



5.2. Exemples

Exemple 15

Voici des exemples basiques.

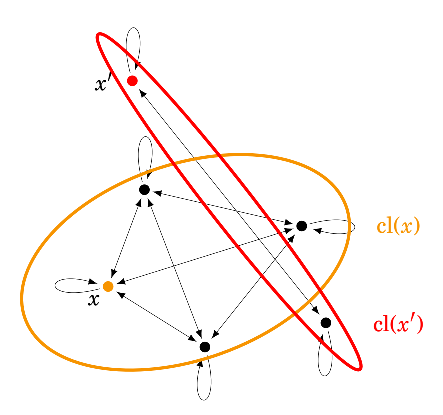
1. La relation $\mathscr{R}$ «être parallèle» est une relation d'équivalence pour l'ensemble E des droites affines du plan.
   - réflexivité : une droite est parallèle à elle-même,
   - symétrie : si D est parallèle à D' alors D' est parallèle à D,
   - transitivité : si D parallèle à D' et D' parallèle à D'' alors D est parallèle à D''.
2. La relation «être du même âge» est une relation d'équivalence.
3. La relation «être perpendiculaire» n'est pas une relation d'équivalence (ni la réflexivité, ni la transitivité ne sont vérifiées).
4. La relation $\leqslant$ (sur $E = \mathbb{R}$ par exemple) n'est pas une relation d'équivalence (la symétrie n'est pas vérifiée).

5.3. Classes d'équivalence

Définition 9

Soit $\mathscr{R}$ une relation d'équivalence sur un ensemble E. Soit $x \in E$, la ***classe d'équivalence*** de x est

$$\mathrm{cl}(x) = \{y \in E \mid y\mathscr{R}x\}$$



$\mathrm{cl}(x)$ est donc un sous-ensemble de E, on le note aussi $\overline{x}$. Si $y \in \mathrm{cl}(x)$, on dit que y un ***représentant*** de $\mathrm{cl}(x)$.

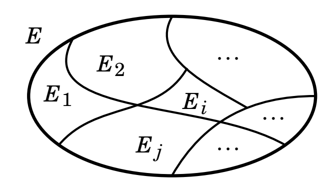
Soit E un ensemble et $\mathscr{R}$ une relation d'équivalence.

Proposition 14

On a les propriétés suivantes :

1. $\mathrm{cl}(x) = \mathrm{cl}(y) \iff x\mathscr{R}y$.
2. Pour tout $x, y \in E$, $\mathrm{cl}(x) = \mathrm{cl}(y)$ ou $\mathrm{cl}(x) \cap \mathrm{cl}(y) = \varnothing$.
3. Soit C un ensemble de représentants de toutes les classes alors $\{\mathrm{cl}(x) \mid x \in C\}$ constitue une partition de E.

Une ***partition*** de E est un ensemble $\{E_i\}$ de parties de E tel que $E = \bigcup_i E_i$ et $E_i \cap E_j = \varnothing$ (si $i \neq j$).



Exemples :

1. Pour la relation «être du même âge», la classe d'équivalence d'une personne est l'ensemble des personnes ayant le même âge. Il y a donc une classe d'équivalence formée des personnes de 19 ans, une autre formée des personnes de 20 ans,... Les trois assertions de la proposition se lisent ainsi :
   - On est dans la même classe d'équivalence si et seulement si on est du même âge.
   - Deux personnes appartiennent soit à la même classe, soit à des classes disjointes.
   - Si on choisit une personne de chaque âge possible, cela forme un ensemble de représentants C. Maintenant une personne quelconque appartient à une et une seule classe d'un des représentants.

2. Pour la relation «être parallèle», la classe d'équivalence d'une droite est l'ensemble des droites parallèles. À chaque classe d'équivalence correspond une et une seule direction.

Voici un exemple que vous connaissez depuis longtemps :

Exemple 16

Définissons sur $E = \mathbb{Z} \times \mathbb{N}^*$ la relation $\mathscr{R}$ par

$$(p,q)\mathscr{R}(p',q') \iff pq' = p'q.$$

Tout d'abord $\mathscr{R}$ est une relation d'équivalence :

- $\mathscr{R}$ est réflexive : pour tout (p,q) on a bien $pq = pq$ et donc $(p,q)\mathscr{R}(p,q)$.
- $\mathscr{R}$ est symétrique : pour tout (p,q), (p',q') tels que $(p,q)\mathscr{R}(p',q')$ on a donc $pq' = p'q$ et donc $p'q = pq'$ d'où $(p',q')\mathscr{R}(p,q)$.
- $\mathscr{R}$ est transitive : pour tout (p,q), (p',q'), (p'',q'') tels que $(p,q)\mathscr{R}(p',q')$ et $(p',q')\mathscr{R}(p'',q'')$ on a donc $pq' = p'q$ et $p'q'' = p''q'$. Alors $(pq')q'' = (p'q)q'' = q(p'q'') = q(p''q')$. En divisant par $q' \neq 0$ on obtient $pq'' = qp''$ et donc $(p,q)\mathscr{R}(p'',q'')$.

Nous allons noter $\frac{p}{q} = \mathrm{cl}(p,q)$ la classe d'équivalence d'un élément $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$. Par exemple, comme $(2,3)\mathscr{R}(4,6)$ (car $2 \times 6 = 3 \times 4$) alors les classes de $(2,3)$ et $(4,6)$ sont égales : avec notre notation cela s'écrit : $\frac{2}{3} = \frac{4}{6}$.

C'est ainsi que l'on définit les rationnels : l'ensemble $\mathbb{Q}$ des rationnels est l'ensemble de classes d'équivalence de la relation $\mathscr{R}$.

Les nombres $\frac{2}{3} = \frac{4}{6}$ sont bien égaux (ce sont les mêmes classes) mais les écritures sont différentes (les représentants sont distincts).

5.4. L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geqslant 2$ un entier. Définissons la relation suivante sur l'ensemble $E = \mathbb{Z}$:

$$\boxed{a \equiv b \pmod n \iff a - b \text{ est un multiple de } n}$$

Exemples pour $n = 7$: $10 \equiv 3 \pmod 7$, $19 \equiv 5 \pmod 7$, $77 \equiv 0 \pmod 7$, $-1 \equiv 20 \pmod 7$.

Cette relation est bien une relation d'équivalence :

- Pour tout $a \in \mathbb{Z}$, $a - a = 0 = 0 \cdot n$ est un multiple de n donc $a \equiv a \pmod n$.
- Pour $a, b \in \mathbb{Z}$ tels que $a \equiv b \pmod n$ alors $a - b$ est un multiple de n, autrement dit il existe $k \in \mathbb{Z}$ tel que $a - b = kn$ et donc $b - a = (-k)n$ et ainsi $b \equiv a \pmod n$.
- Si $a \equiv b \pmod n$ et $b \equiv c \pmod n$ alors il existe $k, k' \in \mathbb{Z}$ tels que $a - b = kn$ et $b - c = k'n$. Alors $a - c = (a - b) + (b - c) = (k + k')n$ et donc $a \equiv c \pmod n$.

La classe d'équivalence de $a \in \mathbb{Z}$ est notée $\overline{a}$. Par définition nous avons donc

$$\overline{a} = \mathrm{cl}(a) = \{b \in \mathbb{Z} \mid b \equiv a \pmod n\}.$$

Comme un tel b s'écrit $b = a + kn$ pour un certain $k \in \mathbb{Z}$ alors c'est aussi exactement

$$\overline{a} = a + n\mathbb{Z} = \{a + kn \mid k \in \mathbb{Z}\}.$$

Comme $n \equiv 0 \pmod n$, $n + 1 \equiv 1 \pmod n$, ... alors

$$\overline{n} = \overline{0}, \quad \overline{n+1} = \overline{1}, \quad \overline{n+2} = \overline{2}, \dots$$

et donc l'ensemble des classes d'équivalence est l'ensemble

$$\boxed{\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}}$$

qui contient exactement n éléments.
Par exemple : pour $n = 7$, $\overline{0} = \{\ldots, -14, -7, 0, 7, 14, 21, \ldots\} = 7\mathbb{Z}$; $\overline{1} = \{\ldots, -13, -6, 1, 8, 15, \ldots\} = 1 + 7\mathbb{Z}$; ... ; $\overline{6} = \{\ldots, -8, -1, 6, 13, 20, \ldots\} = 6 + 7\mathbb{Z}$. Mais ensuite $\overline{7} = \{\ldots - 7, 0, 7, 14, 21, \ldots\} = \overline{0} = 7\mathbb{Z}$. Ainsi $\mathbb{Z}/7\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{6}\right\}$ possède 7 éléments.

Remarque

Dans beaucoup de situations de la vie courante, nous raisonnons avec les modulos. Par exemple pour l'heure : les minutes et les secondes sont modulo 60 (après 59 minutes on repart à zéro), les heures modulo 24 (ou modulo 12 sur le cadran à aiguilles). Les jours de la semaine sont modulo 7, les mois modulo 12,...

Mini-exercices

1. Montrer que la relation définie sur $\mathbb{N}$ par $x \mathscr{R} y \iff \frac{2x+y}{3} \in \mathbb{N}$ est une relation d'équivalence. Montrer qu'il y a 3 classes d'équivalence.
2. Dans $\mathbb{R}^2$ montrer que la relation définie par $(x, y)\mathscr{R}(x', y') \iff x + y' = x' + y$ est une relation d'équivalence. Montrer que deux points (x, y) et (x', y') sont dans une même classe si et seulement s'ils appartiennent à une même droite dont vous déterminerez la direction.
3. On définit une addition sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{p} + \overline{q} = \overline{p+q}$. Calculer la table d'addition dans $\mathbb{Z}/6\mathbb{Z}$ (c'est-à-dire toutes les sommes $\overline{p} + \overline{q}$ pour $\overline{p}, \overline{q} \in \mathbb{Z}/6\mathbb{Z}$). Même chose avec la multiplication $\overline{p} \times \overline{q} = \overline{p \times q}$. Mêmes questions avec $\mathbb{Z}/5\mathbb{Z}$, puis $\mathbb{Z}/8\mathbb{Z}$.

Auteurs

Arnaud Bodin
Benjamin Boutin
Pascal Romon



3 Nombres complexes

Vidéo ■ partie 1. Les nombres complexes, définitions et opérations
Vidéo ■ partie 2. Racines carrées, équation du second degré
Vidéo ■ partie 3. Argument et trigonométrie
Vidéo ■ partie 4. Nombres complexes et géométrie
Exercices ♦ Nombres complexes

Préambule

L'équation $x+5=2$ a ses coefficients dans $\mathbb{N}$ mais pourtant sa solution $x=-3$ n'est pas un entier naturel. Il faut ici considérer l'ensemble plus grand $\mathbb{Z}$ des entiers relatifs.

$$\mathbb{N} \xhookrightarrow{x+5=2} \mathbb{Z} \xhookrightarrow{2x=-3} \mathbb{Q} \xhookrightarrow{x^2=\frac{1}{2}} \mathbb{R} \xhookrightarrow{x^2=-\sqrt{2}} \mathbb{C}$$

De même l'équation $2x=-3$ a ses coefficients dans $\mathbb{Z}$ mais sa solution $x=-\frac{3}{2}$ est dans l'ensemble plus grand des rationnels $\mathbb{Q}$. Continuons ainsi, l'équation $x^2=\frac{1}{2}$ à coefficients dans $\mathbb{Q}$, a ses solutions $x_1=+1/\sqrt{2}$ et $x_2=-1/\sqrt{2}$ dans l'ensemble des réels $\mathbb{R}$. Ensuite l'équation $x^2=-\sqrt{2}$ à ses coefficients dans $\mathbb{R}$ et ses solutions $x_1=+\sqrt{\sqrt{2}}\mathrm{i}$ et $x_2=-\sqrt{\sqrt{2}}\mathrm{i}$ dans l'ensemble des nombres complexes $\mathbb{C}$. Ce processus est-il sans fin ? Non ! Les nombres complexes sont en quelque sorte le bout de la chaîne car nous avons le théorème de d'Alembert-Gauss suivant : « *Pour n'importe quelle équation polynomiale $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0 = 0$ où les coefficients a_i sont des complexes (ou bien des réels), alors les solutions $x_1, \ldots, x_n$ sont dans l'ensemble des nombres complexes* ».

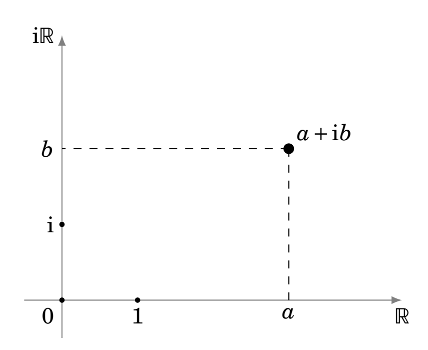
Outre la résolution d'équations, les nombres complexes s'appliquent à la trigonométrie, à la géométrie (comme nous le verrons dans ce chapitre) mais aussi à l'électronique, à la mécanique quantique, etc.

1. Les nombres complexes

1.1. Définition

Définition 10

Un ***nombre complexe*** est un couple $(a,b) \in \mathbb{R}^2$ que l'on notera $a + ib$

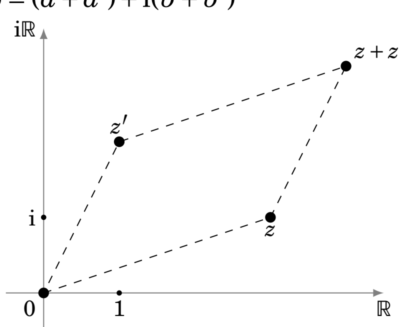


Cela revient à identifier 1 avec le vecteur $(1,0)$ de $\mathbb{R}^2$, et i avec le vecteur $(0,1)$. On note $\mathbb{C}$ l'ensemble des nombres complexes. Si $b = 0$, alors $z = a$ est situé sur l'axe des abscisses, que l'on identifie à $\mathbb{R}$. Dans ce cas on dira que z est ***réel***, et $\mathbb{R}$ apparaît comme un sous-ensemble de $\mathbb{C}$, appelé ***axe réel***. Si $b \neq 0$, z est dit ***imaginaire*** et si $b \neq 0$ et $a = 0$, z est dit ***imaginaire pur***.

1.2. Opérations

Si $z = a + ib$ et $z' = a' + ib'$ sont deux nombres complexes, alors on définit les opérations suivantes :

- ***addition*** : $(a + ib) + (a' + ib') = (a + a') + i(b + b')$

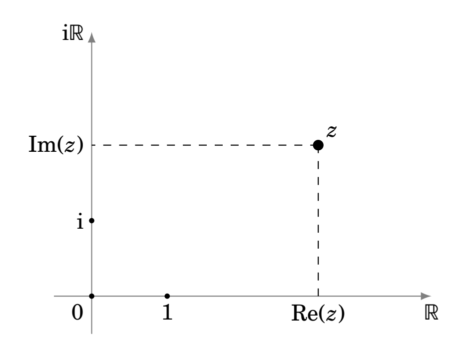


- ***multiplication*** : $(a + ib) \times (a' + ib') = (aa' - bb') + i(ab' + ba')$. C'est la multiplication usuelle avec la convention suivante :

$$i^2 = -1$$

1.3. Partie réelle et imaginaire

Soit $z = a + ib$ un nombre complexe, sa ***partie réelle*** est le réel a et on la note $\text{Re}(z)$; sa ***partie imaginaire*** est le réel b et on la note $\text{Im}(z)$.



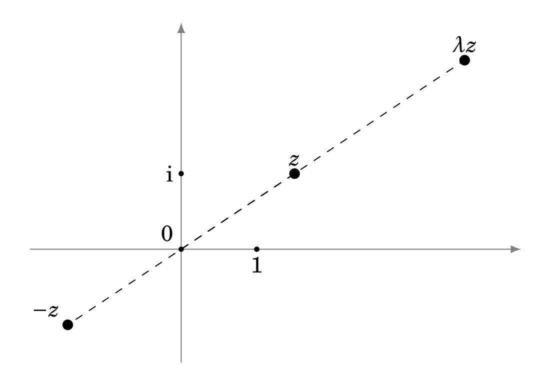
Par identification de $\mathbb{C}$ à $\mathbb{R}^2$, l'écriture $z = \mathrm{Re}(z) + \mathrm{i}\,\mathrm{Im}(z)$ est unique :

$$z = z' \iff \begin{cases} \mathrm{Re}(z) = \mathrm{Re}(z') \\ \text{et} \\ \mathrm{Im}(z) = \mathrm{Im}(z') \end{cases}$$

En particulier un nombre complexe est réel si et seulement si sa partie imaginaire est nulle. Un nombre complexe est nul si et et seulement si sa partie réelle et sa partie imaginaire sont nuls.

1.4. Calculs

Quelques définitions et calculs sur les nombres complexes.



- L'***opposé*** de $z = a + \mathrm{i}b$ est $-z = (-a) + \mathrm{i}(-b) = -a - \mathrm{i}b$.
- La ***multiplication par un scalaire*** $\lambda \in \mathbb{R}$: $\lambda \cdot z = (\lambda a) + \mathrm{i}(\lambda b)$.
- L'***inverse*** : si $z \neq 0$, il existe un unique $z' \in \mathbb{C}$ tel que $zz' = 1$ (où $1 = 1 + \mathrm{i} \times 0$).
  Pour la preuve et le calcul on écrit $z = a + \mathrm{i}b$ puis on cherche $z' = a' + \mathrm{i}b'$ tel que $zz' = 1$. Autrement dit $(a + \mathrm{i}b)(a' + \mathrm{i}b') = 1$. En développant et identifiant les parties réelles et imaginaires on obtient les équations

  $$\begin{cases} aa' - bb' = 1 & (L_1) \\ ab' + ba' = 0 & (L_2) \end{cases}$$

  En écrivant $aL_1 + bL_2$ (on multiplie la ligne (L_1) par a, la ligne (L_2) par b et on additionne) et $-bL_1 + aL_2$ on en déduit

  $$\begin{cases} a'\left(a^2 + b^2\right) = a \\ b'\left(a^2 + b^2\right) = -b \end{cases} \quad \text{donc} \quad \begin{cases} a' = \frac{a}{a^2+b^2} \\ b' = -\frac{b}{a^2+b^2} \end{cases}$$

  L'inverse de z est donc

  $$z' = \frac{1}{z} = \frac{a}{a^2 + b^2} + \mathrm{i}\frac{-b}{a^2 + b^2} = \frac{a - \mathrm{i}b}{a^2 + b^2}.$$
- La ***division*** : $\frac{z}{z'}$ est le nombre complexe $z \times \frac{1}{z'}$.
- Propriété d'intégrité : si $zz' = 0$ alors $z = 0$ ou $z' = 0$.
- Puissances : $z^2 = z \times z$, $z^n = z \times \cdots \times z$ (n fois, $n \in \mathbb{N}$). Par convention $z^0 = 1$ et $z^{-n} = \left(\frac{1}{z}\right)^n = \frac{1}{z^n}$.

Proposition 15

Pour tout $z \in \mathbb{C}$ différent de 1

$$1+z+z^2+\cdots+z^n = \frac{1-z^{n+1}}{1-z}.$$

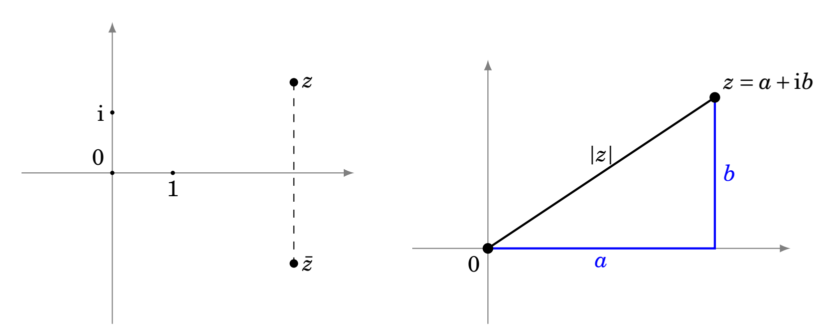
La preuve est simple : notons $S = 1+z+z^2+\cdots+z^n$, alors en développant $S\cdot(1-z)$ presque tous les termes se télescopent et l'on trouve $S\cdot(1-z) = 1-z^{n+1}$.

Remarque

Il n'y pas d'ordre naturel sur $\mathbb{C}$, il ne faut donc jamais écrire $z \geqslant 0$ ou $z \leqslant z'$.

1.5. Conjugué, module

Le ***conjugué*** de $z = a+ib$ est $\bar{z} = a-ib$, autrement dit $\mathrm{Re}(\bar{z}) = \mathrm{Re}(z)$ et $\mathrm{Im}(\bar{z}) = -\mathrm{Im}(z)$. Le point $\bar{z}$ est le symétrique du point z par rapport à l'axe réel.
Le ***module*** de $z = a+ib$ est le réel positif $|z| = \sqrt{a^2+b^2}$. Comme $z\times\bar{z} = (a+ib)(a-ib) = a^2+b^2$ alors le module vaut aussi $|z| = \sqrt{z\bar{z}}$.



Quelques formules :

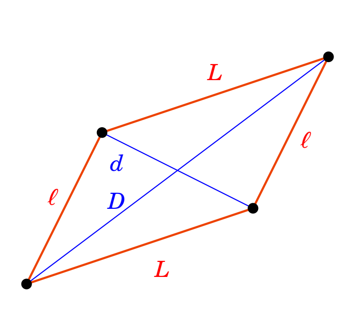
- $\overline{z+z'} = \bar{z}+\overline{z'}$, $\bar{\bar{z}} = z$, $\overline{zz'} = \bar{z}\overline{z'}$
- $z = \bar{z} \iff z \in \mathbb{R}$
- $|z|^2 = z\times\bar{z}$, $|\bar{z}| = |z|$, $|zz'| = |z||z'|$
- $|z| = 0 \iff z = 0$
- L'inégalité triangulaire : $|z+z'| \leqslant |z|+|z'|$

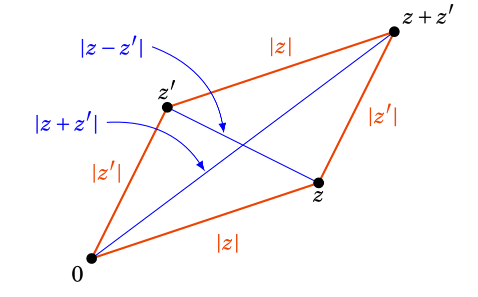
Exemple 17

Dans un parallélogramme, la somme des carrés des diagonales égale la somme des carrés des côtés.

Si les longueurs des côtés sont notées L et ℓ et les longueurs des diagonales sont D et d alors il s'agit de montrer l'égalité

$$D^2 + d^2 = 2\ell^2 + 2L^2.$$





Démonstration

Cela devient simple si l'on considère que notre parallélogramme a pour sommets $0, z, z'$ et le dernier sommet est donc $z + z'$. La longueur du grand côté est ici $|z|$, celle du petit côté est $|z'|$. La longueur de la grande diagonale est $|z + z'|$. Enfin il faut se convaincre que la longueur de la petite diagonale est $|z - z'|$.

$$\begin{aligned}
D^2 + d^2 = \left|z + z'\right|^2 + \left|z - z'\right|^2 &= \left(z + z'\right)\overline{(z + z')} + \left(z - z'\right)\overline{(z - z')} \\
&= z\bar{z} + z\overline{z'} + z'\bar{z} + z'\overline{z'} + z\bar{z} - z\overline{z'} - z'\bar{z} + z'\overline{z'} \\
&= 2z\bar{z} + 2z'\overline{z'} = 2|z|^2 + 2\left|z'\right|^2 \\
&= 2\ell^2 + 2L^2
\end{aligned}$$

Mini-exercices

1. Calculer $1 - 2\mathrm{i} + \frac{\mathrm{i}}{1-2\mathrm{i}}$.
2. Écrire sous la forme $a + ib$ les nombres complexes $(1+\mathrm{i})^2$, $(1+\mathrm{i})^3$, $(1+\mathrm{i})^4$, $(1+\mathrm{i})^8$.
3. En déduire $1 + (1+\mathrm{i}) + (1+\mathrm{i})^2 + \cdots + (1+\mathrm{i})^7$.
4. Soit $z \in \mathbb{C}$ tel que $|1 + \mathrm{i}z| = |1 - \mathrm{i}z|$, montrer que $z \in \mathbb{R}$.
5. Montrer que si $|\mathrm{Re}\, z| \leqslant |\mathrm{Re}\, z'|$ et $|\mathrm{Im}\, z| \leqslant |\mathrm{Im}\, z'|$ alors $|z| \leqslant |z'|$, mais que la réciproque est fausse.
6. Montrer que $1/\bar{z} = z/|z|^2$ (pour $z \neq 0$).

2. Racines carrées, équation du second degré

2.1. Racines carrées d'un nombre complexe

Pour $z \in \mathbb{C}$, une ***racine carrée*** est un nombre complexe ω tel que $\omega^2 = z$.
Par exemple si $x \in \mathbb{R}_+$, on connaît deux racines carrées : $\sqrt{x}, -\sqrt{x}$. Autre exemple : les racines carrées de -1 sont i et $-\mathrm{i}$.

Proposition 16

Soit z un nombre complexe, alors z admet deux racines carrées, ω et $-\omega$.

Attention ! Contrairement au cas réel, il n'y a pas de façon privilégiée de choisir une racine plutôt que l'autre, donc pas de fonction racine. On ne dira donc jamais « soit ω la racine de z ».

Si $z \neq 0$ ces deux racines carrées sont distinctes. Si $z = 0$ alors $\omega = 0$ est une racine double.
Pour $z = a + ib$ nous allons calculer ω et $-\omega$ en fonction de a et b.

Démonstration

Nous écrivons $\omega = x + \mathrm{i}y$, nous cherchons x, y tels que $\omega^2 = z$.

$$\begin{aligned} \omega^2 = z &\iff (x+\mathrm{i}y)^2 = a + \mathrm{i}b \\ &\iff \begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases} \quad \text{en identifiant parties réelles et parties imaginaires.} \end{aligned}$$

Petite astuce ici : nous rajoutons l'équation $|\omega|^2 = |z|$ (qui se déduit bien sûr de $\omega^2 = z$) qui s'écrit aussi $x^2 + y^2 = \sqrt{a^2+b^2}$. Nous obtenons des systèmes équivalents aux précédents :

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \\ x^2 + y^2 = \sqrt{a^2+b^2} \end{cases} \iff \begin{cases} 2x^2 = \sqrt{a^2+b^2} + a \\ 2y^2 = \sqrt{a^2+b^2} - a \\ 2xy = b \end{cases} \iff \begin{cases} x = \pm\frac{1}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}+a} \\ y = \pm\frac{1}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}-a} \\ 2xy = b \end{cases}$$

Discutons suivant le signe du réel b. Si $b \geqslant 0$, x et y sont de même signe ou nuls (car $2xy = b \geqslant 0$) donc

$$\omega = \pm\frac{1}{\sqrt{2}}\left(\sqrt{\sqrt{a^2+b^2}+a} + \mathrm{i}\sqrt{\sqrt{a^2+b^2}-a}\right),$$

et si $b \leqslant 0$

$$\omega = \pm\frac{1}{\sqrt{2}}\left(\sqrt{\sqrt{a^2+b^2}+a} - \mathrm{i}\sqrt{\sqrt{a^2+b^2}-a}\right).$$

En particulier si $b = 0$ le résultat dépend du signe de a, si $a \geqslant 0$, $\sqrt{a^2} = a$ et par conséquent $\omega = \pm\sqrt{a}$, tandis que si $a < 0$, $\sqrt{a^2} = -a$ et donc $\omega = \pm\mathrm{i}\sqrt{-a} = \pm\mathrm{i}\sqrt{|a|}$.

Il n'est pas nécessaire d'apprendre ces formules mais il est indispensable de savoir refaire les calculs.

Exemple 18

Les racines carrées de i sont $+\frac{\sqrt{2}}{2}(1+\mathrm{i})$ et $-\frac{\sqrt{2}}{2}(1+\mathrm{i})$.
En effet :

$$\begin{aligned} \omega^2 = \mathrm{i} &\iff (x+\mathrm{i}y)^2 = \mathrm{i} \\ &\iff \begin{cases} x^2 - y^2 = 0 \\ 2xy = 1 \end{cases} \end{aligned}$$

Rajoutons la conditions $|\omega|^2 = |\mathrm{i}|$ pour obtenir le système équivalent au précédent :

$$\begin{cases} x^2 - y^2 = 0 \\ 2xy = 1 \\ x^2 + y^2 = 1 \end{cases} \iff \begin{cases} 2x^2 = 1 \\ 2y^2 = 1 \\ 2xy = 1 \end{cases} \iff \begin{cases} x = \pm\frac{1}{\sqrt{2}} \\ y = \pm\frac{1}{\sqrt{2}} \\ 2xy = 1 \end{cases}$$

Les réels x et y sont donc de même signe, nous trouvons bien deux solutions :

$$x + \mathrm{i}y = \frac{1}{\sqrt{2}} + \mathrm{i}\frac{1}{\sqrt{2}} \quad \text{ou} \quad x + \mathrm{i}y = -\frac{1}{\sqrt{2}} - \mathrm{i}\frac{1}{\sqrt{2}}$$

2.2. Équation du second degré

Proposition 17

L'équation du second degré $az^2 + bz + c = 0$, où $a, b, c \in \mathbb{C}$ et $a \neq 0$, possède deux solutions $z_1, z_2 \in \mathbb{C}$ éventuellement confondues.
Soit $\Delta = b^2 - 4ac$ le discriminant et $\delta \in \mathbb{C}$ une racine carrée de Δ. Alors les solutions sont

$$\boxed{z_1 = \frac{-b+\delta}{2a} \quad \text{et} \quad z_2 = \frac{-b-\delta}{2a}.}$$

Et si $\Delta = 0$ alors la solution $z = z_1 = z_2 = -b/2a$ est unique (elle est dite double). Si on s'autorisait à écrire $\delta = \sqrt{\Delta}$ pour le nombre complexe Δ, on obtiendrait la même formule que celle que vous connaissez lorsque a, b, c sont réels.

Exemple 19

- $z^2 + z + 1 = 0$, $\Delta = -3$, $\delta = \mathrm{i}\sqrt{3}$, les solutions sont $z = \dfrac{-1 \pm \mathrm{i}\sqrt{3}}{2}$.
- $z^2 + z + \frac{1-\mathrm{i}}{4} = 0$, $\Delta = \mathrm{i}$, $\delta = \frac{\sqrt{2}}{2}(1+\mathrm{i})$, les solutions sont $z = \dfrac{-1 \pm \frac{\sqrt{2}}{2}(1+\mathrm{i})}{2} = -\frac{1}{2} \pm \frac{\sqrt{2}}{4}(1+\mathrm{i})$.

On retrouve aussi le résultat bien connu pour le cas des équations à coefficients réels :

Corollaire 1

Si les coefficients a, b, c sont réels alors $\Delta \in \mathbb{R}$ et les solutions sont de trois types :
- si $\Delta = 0$, la racine double est réelle et vaut $-\dfrac{b}{2a}$,
- si $\Delta > 0$, on a deux solutions réelles $\dfrac{-b \pm \sqrt{\Delta}}{2a}$,
- si $\Delta < 0$, on a deux solutions complexes, mais non réelles, $\dfrac{-b \pm \mathrm{i}\sqrt{-\Delta}}{2a}$.

Démonstration

On écrit la factorisation

$$\begin{aligned}
az^2 + bz + c &= a\left(z^2 + \frac{b}{a}z + \frac{c}{a}\right) = a\left(\left(z + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right) \\
&= a\left(\left(z + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right) = a\left(\left(z + \frac{b}{2a}\right)^2 - \frac{\delta^2}{4a^2}\right) \\
&= a\left(\left(z + \frac{b}{2a}\right) - \frac{\delta}{2a}\right)\left(\left(z + \frac{b}{2a}\right) + \frac{\delta}{2a}\right) \\
&= a\left(z - \frac{-b+\delta}{2a}\right)\left(z - \frac{-b-\delta}{2a}\right) = a(z - z_1)(z - z_2)
\end{aligned}$$

Donc le binôme s'annule si et seulement si $z = z_1$ ou $z = z_2$.

2.3. Théorème fondamental de l'algèbre

Théorème 2. d'Alembert–Gauss

Soit $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ un polynôme à coefficients complexes et de degré n. Alors l'équation $P(z) = 0$ admet exactement n solutions complexes comptées avec leur multiplicité.
En d'autres termes il existe des nombres complexes $z_1, \ldots, z_n$ (dont certains sont éventuellement confondus) tels que

$$P(z) = a_n(z - z_1)(z - z_2)\cdots(z - z_n).$$

Nous admettons ce théorème.

Mini-exercices

1. Calculer les racines carrées de $-\mathrm{i}$, $3 - 4\mathrm{i}$.
2. Résoudre les équations : $z^2 + z - 1 = 0$, $2z^2 + (-10 - 10\mathrm{i})z + 24 - 10\mathrm{i} = 0$.
3. Résoudre l'équation $z^2 + (\mathrm{i} - \sqrt{2})z - \mathrm{i}\sqrt{2}$, puis l'équation $Z^4 + (\mathrm{i} - \sqrt{2})Z^2 - \mathrm{i}\sqrt{2}$.
4. Montrer que si $P(z) = z^2 + bz + c$ possède pour racines $z_1, z_2 \in \mathbb{C}$ alors $z_1 + z_2 = -b$ et $z_1 \cdot z_2 = c$.
5. Trouver les paires de nombres dont la somme vaut i et le produit 1.
6. Soit $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0$ avec $a_i \in \mathbb{R}$ pour tout i. Montrer que si z est racine de P alors $\bar{z}$ aussi.

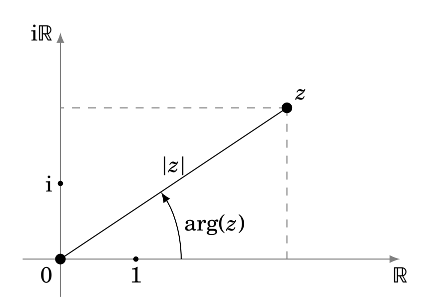
3. Argument et trigonométrie

3.1. Argument

Si $z = x + iy$ est de module 1, alors $x^2 + y^2 = |z|^2 = 1$. Par conséquent le point (x, y) est sur le cercle unité du plan, et son abscisse x est notée $\cos\theta$, son ordonnée y est $\sin\theta$, où θ est (une mesure de) l'angle entre l'axe réel et z. Plus généralement, si $z \neq 0$, $z/|z|$ est de module 1, et cela amène à :

Définition 11

Pour tout $z \in \mathbb{C}^* = \mathbb{C} - \{0\}$, un nombre $\theta \in \mathbb{R}$ tel que $z = |z|(\cos\theta + \mathrm{i}\sin\theta)$ est appelé un ***argument*** de z et noté $\theta = \arg(z)$.



Cet argument est défini modulo 2π. On peut imposer à cet argument d'être unique si on rajoute la condition $\theta \in]-\pi, +\pi]$.

Remarque

$$\theta \equiv \theta' \pmod{2\pi} \iff \exists k \in \mathbb{Z}, \theta = \theta' + 2k\pi \iff \begin{cases} \cos\theta = \cos\theta' \\ \sin\theta = \sin\theta' \end{cases}$$

Proposition 18

L'argument satisfait les propriétés suivantes :

- $\arg(zz') \equiv \arg(z) + \arg(z') \pmod{2\pi}$
- $\arg(z^n) \equiv n\arg(z) \pmod{2\pi}$
- $\arg(1/z) \equiv -\arg(z) \pmod{2\pi}$
- $\arg(\bar{z}) \equiv -\arg z \pmod{2\pi}$

Démonstration

$$\begin{aligned} zz' &= |z|(\cos\theta + i\sin\theta)|z'|(\cos\theta' + i\sin\theta') \\ &= |zz'|(\cos\theta\cos\theta' - \sin\theta\sin\theta' + i(\cos\theta\sin\theta' + \sin\theta\cos\theta')) \\ &= |zz'|(\cos(\theta+\theta') + i\sin(\theta+\theta')) \end{aligned}$$

donc $\arg(zz') \equiv \arg(z) + \arg(z') \pmod{2\pi}$. On en déduit les deux autres propriétés, dont la deuxième par récurrence.

3.2. Formule de Moivre, notation exponentielle

La ***formule de Moivre*** est :

$$\boxed{(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)}$$

Démonstration

Par récurrence, on montre que

$$\begin{aligned} (\cos\theta + i\sin\theta)^n &= (\cos\theta + i\sin\theta)^{n-1} \times (\cos\theta + i\sin\theta) \\ &= (\cos((n-1)\theta) + i\sin((n-1)\theta)) \times (\cos\theta + i\sin\theta) \\ &= (\cos((n-1)\theta)\cos\theta - \sin((n-1)\theta)\sin\theta) \\ &\quad + i(\cos((n-1)\theta)\sin\theta + \sin((n-1)\theta)\cos\theta) \\ &= \cos n\theta + i\sin n\theta \end{aligned}$$

Nous définissons la ***notation exponentielle*** par

$$\boxed{e^{i\theta} = \cos\theta + i\sin\theta}$$

et donc tout nombre complexe s'écrit

$$\boxed{z = \rho e^{i\theta}}$$

où $\rho = |z|$ est le module et $\theta = \arg(z)$ est un argument.

Avec la notation exponentielle, on peut écrire pour $z = \rho e^{i\theta}$ et $z' = \rho' e^{i\theta'}$

$$\begin{cases} zz' = \rho\rho' e^{i\theta} e^{i\theta'} = \rho\rho' e^{i(\theta+\theta')} \\ z^n = \left(\rho e^{i\theta}\right)^n = \rho^n \left(e^{i\theta}\right)^n = \rho^n e^{in\theta} \\ 1/z = 1/\left(\rho e^{i\theta}\right) = \frac{1}{\rho} e^{-i\theta} \\ \bar{z} = \rho e^{-i\theta} \end{cases}$$

La formule de Moivre se réduit à l'égalité : $\left(e^{i\theta}\right)^n = e^{in\theta}$.
Et nous avons aussi : $\rho e^{i\theta} = \rho' e^{i\theta'}$ (avec $\rho, \rho' > 0$) si et seulement si $\rho = \rho'$ et $\theta \equiv \theta' \pmod{2\pi}$.

3.3. Racines n-ième

Définition 12

Pour $z \in \mathbb{C}$ et $n \in \mathbb{N}$, une ***racine n-ième*** est un nombre $\omega \in \mathbb{C}$ tel que $\omega^n = z$.

Proposition 19

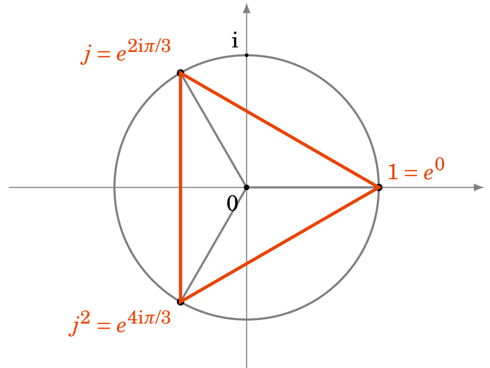
Il y a n racines n-ièmes $\omega_0, \omega_1, \ldots, \omega_{n-1}$ de $z = \rho e^{i\theta}$, ce sont :

$$\boxed{\omega_k = \rho^{1/n} e^{\frac{i\theta + 2ik\pi}{n}}, \quad k = 0, 1, \ldots, n-1}$$

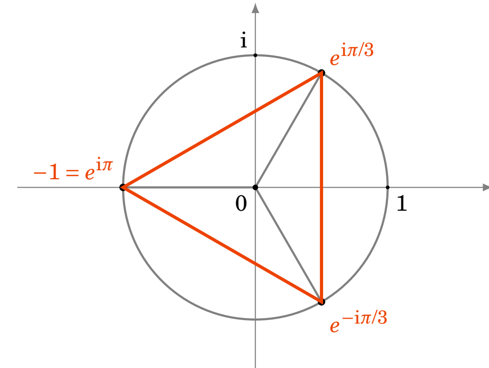
Démonstration

Écrivons $z = \rho e^{i\theta}$ et cherchons ω sous la forme $\omega = re^{it}$ tel que $z = \omega^n$. Nous obtenons donc $\rho e^{i\theta} = \omega^n = \left(re^{it}\right)^n = r^n e^{int}$. Prenons tout d'abord le module : $\rho = \left|\rho e^{i\theta}\right| = \left|r^n e^{int}\right| = r^n$ et donc $r = \rho^{1/n}$ (il s'agit ici de nombres réels). Pour les arguments nous avons $e^{int} = e^{i\theta}$ et donc $nt \equiv \theta \pmod{2\pi}$ (n'oubliez surtout pas le modulo 2π !). Ainsi on résout $nt = \theta + 2k\pi$ (pour $k \in \mathbb{Z}$) et donc $t = \frac{\theta}{n} + \frac{2k\pi}{n}$. Les solutions de l'équation $\omega^n = z$ sont donc les $\omega_k = \rho^{1/n} e^{\frac{i\theta+2ik\pi}{n}}$. Mais en fait il n'y a que n solutions distinctes car $\omega_n = \omega_0$, $\omega_{n+1} = \omega_1$, ... Ainsi les n solutions sont $\omega_0, \omega_1, \ldots, \omega_{n-1}$.

Par exemple pour $z = 1$, on obtient les n ***racines n-ièmes de l'unité*** $e^{2ik\pi/n}$, $k = 0, \ldots, n-1$ qui forment un groupe multiplicatif.

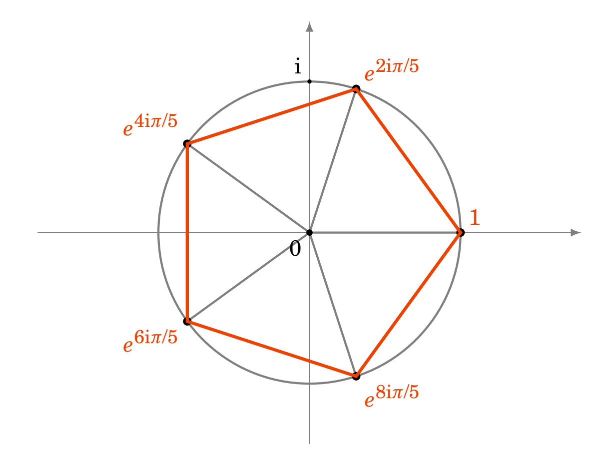


Racine 3-ième de l'unité ($z = 1$, $n = 3$)



Racine 3-ième de -1 ($z = -1$, $n = 3$)

Les racines 5-ième de l'unité ($z = 1$, $n = 5$) forment un pentagone régulier :



3.4. Applications à la trigonométrie

Voici les ***formules d'Euler***, pour $\theta \in \mathbb{R}$:

$$\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2} \quad , \quad \sin\theta = \frac{e^{i\theta}-e^{-i\theta}}{2i}$$

Ces formules s'obtiennent facilement en utilisant la définition de la notation exponentielle. Nous les appliquons dans la suite à deux problèmes : le développement et la linéarisation.

Développement. On exprime $\sin n\theta$ ou $\cos n\theta$ en fonction des puissances de $\cos\theta$ et $\sin\theta$.

Méthode : on utilise la formule de Moivre pour écrire $\cos(n\theta)+i\sin(n\theta) = (\cos\theta + i\sin\theta)^n$ que l'on développe avec la formule du binôme de Newton.

Exemple 20

$$\begin{aligned}
\cos 3\theta + i\sin 3\theta &= (\cos\theta + i\sin\theta)^3 \\
&= \cos^3\theta + 3i\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta \\
&= \left(\cos^3\theta - 3\cos\theta\sin^2\theta\right) + i\left(3\cos^2\theta\sin\theta - \sin^3\theta\right)
\end{aligned}$$

En identifiant les parties réelles et imaginaires, on déduit que

$$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta \quad \text{et} \quad \sin 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta.$$

Linéarisation. On exprime $\cos^n\theta$ ou $\sin^n\theta$ en fonction des $\cos k\theta$ et $\sin k\theta$ pour k allant de 0 à n.

Méthode : avec la formule d'Euler on écrit $\sin^n\theta = \left(\frac{e^{i\theta}-e^{-i\theta}}{2i}\right)^n$. On développe à l'aide du binôme de Newton puis on regroupe les termes par paires conjuguées.

Exemple 21

$$
\begin{aligned}
\sin^3\theta &= \left(\frac{e^{i\theta}-e^{-i\theta}}{2i}\right)^3 \\
&= \frac{1}{-8i}\left((e^{i\theta})^3 - 3(e^{i\theta})^2 e^{-i\theta} + 3e^{i\theta}(e^{-i\theta})^2 - (e^{-i\theta})^3\right) \\
&= \frac{1}{-8i}\left(e^{3i\theta} - 3e^{i\theta} + 3e^{-i\theta} - e^{-3i\theta}\right) \\
&= -\frac{1}{4}\left(\frac{e^{3i\theta}-e^{-3i\theta}}{2i} - 3\frac{e^{i\theta}-e^{-i\theta}}{2i}\right) \\
&= -\frac{\sin 3\theta}{4} + \frac{3\sin\theta}{4}
\end{aligned}
$$

3.5. Mini-exercices

Mini-exercices

1. Mettre les nombres suivants sont la forme module-argument (avec la notation exponentielle) : 1, i, -1, $-i$, $3i$, $1+i$, $\sqrt{3}-i$, $\overline{\sqrt{3}-i}$, $\frac{1}{\sqrt{3}-i}$, $(\sqrt{3}-i)^{20xx}$ où $20xx$ est l'année en cours.
2. Calculer les racines 5-ième de i.
3. Calculer les racines carrées de $\frac{\sqrt{3}}{2}+\frac{i}{2}$ de deux façons différentes. En déduire les valeurs de $\cos\frac{\pi}{12}$ et $\sin\frac{\pi}{12}$.
4. Donner sans calcul la valeur de $\omega_0+\omega_1+\cdots+\omega_{n-1}$, où les ω_i sont les racines n-ième de 1.
5. Développer $\cos(4\theta)$; linéariser $\cos^4\theta$; calculer une primitive de $\theta\mapsto\cos^4\theta$.

4. Nombres complexes et géométrie

On associe bijectivement à tout point M du plan affine $\mathbb{R}^2$ de coordonnées (x,y), le nombre complexe $z=x+iy$ appelé son ***affixe***.

4.1. Équation complexe d'une droite

Soit

$$ax+by=c$$

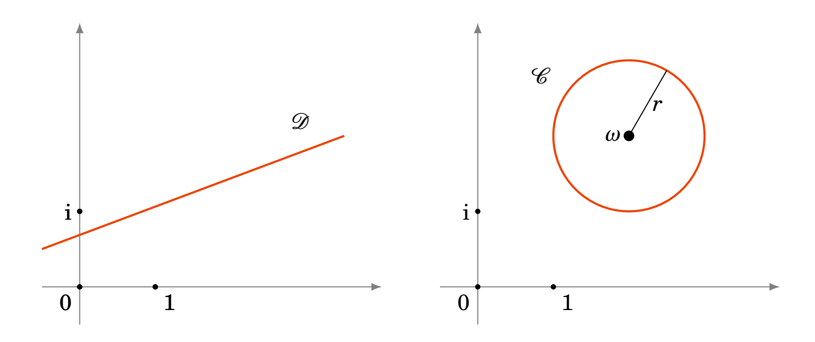
l'équation réelle d'une droite $\mathcal{D}$: a,b,c sont des nombres réels (a et b n'étant pas tous les deux nuls) d'inconnues $(x,y)\in\mathbb{R}^2$.
Écrivons $z=x+iy\in\mathbb{C}$, alors

$$x=\frac{z+\bar{z}}{2},\qquad y=\frac{z-\bar{z}}{2i},$$

donc $\mathcal{D}$ a aussi pour équation $a(z+\bar{z})-ib(z-\bar{z})=2c$ ou encore $(a-ib)z+(a+ib)\bar{z}=2c$. Posons $\omega=a+ib\in\mathbb{C}^*$ et $k=2c\in\mathbb{R}$ alors l'équation complexe d'une droite est :

$$\boxed{\bar{\omega}z+\omega\bar{z}=k}$$

où $\omega\in\mathbb{C}^*$ et $k\in\mathbb{R}$.



4.2. Équation complexe d'un cercle

Soit $\mathscr{C}(\Omega, r)$ le cercle de centre Ω et de rayon r. C'est l'ensemble des points M tel que $\mathrm{dist}(\Omega, M) = r$. Si l'on note ω l'affixe de Ω et z l'affixe de M. Nous obtenons :

$$\mathrm{dist}(\Omega, M) = r \iff |z-\omega| = r \iff |z-\omega|^2 = r^2 \iff (z-\omega)\overline{(z-\omega)} = r^2$$

et en développant nous trouvons que l'équation complexe du cercle centré en un point d'affixe ω et de rayon r est :

$$\boxed{z\bar{z} - \bar{\omega}z - \omega\bar{z} = r^2 - |\omega|^2}$$

où $\omega \in \mathbb{C}$ et $r \in \mathbb{R}$.

4.3. Équation $\frac{|z-a|}{|z-b|} = k$

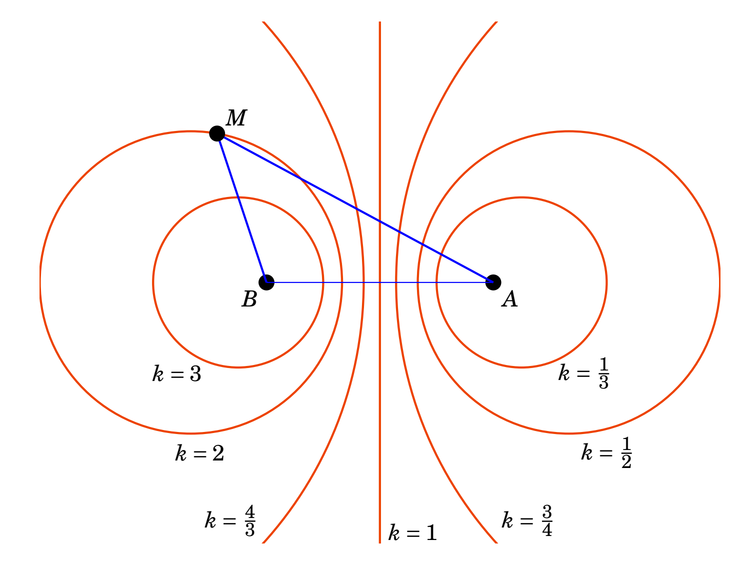
Proposition 20

Soit A, B deux points du plan et $k \in \mathbb{R}_+$. L'ensemble des points M tel que $\frac{MA}{MB} = k$ est

- une droite qui est la médiatrice de $[AB]$, si $k = 1$,
- un cercle, sinon.

Exemple 22

Prenons A le point d'affixe $+1$,B le point d'affixe -1. Voici les figures pour plusieurs valeurs de k.
Par exemple pour $k = 2$ le point M dessiné vérifie bien $MA = 2MB$.



Démonstration

Si les affixes de A,B,M sont respectivement a,b,z, cela revient à résoudre l'équation $\frac{|z-a|}{|z-b|}=k$.

$$\begin{aligned}\frac{|z-a|}{|z-b|}=k &\iff |z-a|^2=k^2|z-b|^2\\ &\iff (z-a)\overline{(z-a)}=k^2(z-b)\overline{(z-b)}\\ &\iff (1-k^2)z\bar{z}-z(\bar{a}-k^2\bar{b})-\bar{z}(a-k^2b)+|a|^2-k^2|b|^2=0\end{aligned}$$

Donc si $k=1$, on pose $\omega=a-k^2b$ et l'équation obtenue $z\bar{\omega}+\bar{z}\omega=|a|^2-k^2|b|^2$ est bien celle d'une droite. Et bien sûr l'ensemble des points qui vérifient $MA=MB$ est la médiatrice de $[AB]$. Si $k\neq 1$ on pose $\omega=\frac{a-k^2b}{1-k^2}$ alors l'équation obtenue est $z\bar{z}-z\bar{\omega}-\bar{z}\omega=\frac{-|a|^2+k^2|b|^2}{1-k^2}$. C'est l'équation d'un cercle de centre ω et de rayon r satisfaisant $r^2-|\omega|^2=\frac{-|a|^2+k^2|b|^2}{1-k^2}$, soit $r^2=\frac{|a-k^2b|^2}{(1-k^2)^2}+\frac{-|a|^2+k^2|b|^2}{1-k^2}$.

Ces calculs se refont au cas par cas, il n'est pas nécessaire d'apprendre les formules.

Mini-exercices

1. Calculer l'équation complexe de la droite passant par 1 et i.
2. Calculer l'équation complexe du cercle de centre $1+2\mathrm{i}$ passant par i.
3. Calculer l'équation complexe des solutions de $\dfrac{|z-\mathrm{i}|}{|z-1|}=1$, puis dessiner les solutions.
4. Même question avec $\dfrac{|z-\mathrm{i}|}{|z-1|}=2$.

Auteurs

Arnaud Bodin
Benjamin Boutin
Pascal Romon





4 Arithmétique

Vidéo ■ partie 1. Division euclidienne et pgcd
Vidéo ■ partie 2. Théorème de Bézout
Vidéo ■ partie 3. Nombres premiers
Vidéo ■ partie 4. Congruences
Exercices ♦ Arithmétique dans $\mathbb{Z}$

Préambule

Une motivation : l'arithmétique est au cœur du cryptage des communication. Pour crypter un message on commence par le transformer en un –ou plusieurs– nombres. Le processus de codage et décodage fait appel à plusieurs notions de ce chapitre :

– On choisit deux ***nombres premiers*** p et q que l'on garde secrets et on pose $n = p \times q$. Le principe étant que même connaissant n il est très difficile de retrouver p et q (qui sont des nombres ayant des centaines de chiffres).
– La clé secrète et la clé publique se calculent à l'aide de l'***algorithme d'Euclide*** et des ***coefficients de Bézout***.
– Les calculs de cryptage se feront ***modulo*** n.
– Le décodage fonctionne grâce à une variante du ***petit théorème de Fermat***.

1. Division euclidienne et pgcd

1.1. Divisibilité et division euclidienne

Définition 13

Soient $a, b \in \mathbb{Z}$. On dit que b ***divise*** a et on note $b|a$ s'il existe $q \in \mathbb{Z}$ tel que

$$\boxed{a = bq}$$

.

Exemple 23

- $7|21$; $6|48$; a est pair si et seulement si $2|a$.
- Pour tout $a \in \mathbb{Z}$ on a $a|0$ et aussi $1|a$.
- Si $a|1$ alors $a = +1$ ou $a = -1$.
- $(a|b$ et $b|a) \implies b = \pm a$.
- $(a|b$ et $b|c) \implies a|c$.
- $(a|b$ et $a|c) \implies a|b+c$.

Théorème 3. Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N} \setminus \{0\}$. Il ***existe*** des entiers $q, r \in \mathbb{Z}$ tels que

$$\boxed{a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b}$$

De plus q et r sont ***uniques***.

Nous avons donc l'équivalence : $r = 0$ si et seulement si b divise a.

Exemple 24

Pour calculer q et r on pose la division «classique». Si $a = 6789$ et $b = 34$ alors

$$6789 = 34 \times 199 + 23$$

On a bien $0 \leqslant 23 < 34$ (sinon c'est que l'on n'a pas été assez loin dans les calculs).

6789	34
34	
338	199
306	
329	
306	
23	

dividende	diviseur
reste	quotient

Démonstration

Existence. On peut supposer $a \geqslant 0$ pour simplifier. Soit $\mathcal{N} = \{n \in \mathbb{N} \mid bn \leqslant a\}$. C'est un ensemble non vide car $n = 0 \in \mathcal{N}$. De plus pour $n \in \mathcal{N}$, on a $n \leqslant a$. Il y a donc un nombre fini d'éléments dans $\mathcal{N}$, notons $q = \max \mathcal{N}$ le plus grand élément.
Alors $qb \leqslant a$ car $q \in \mathcal{N}$, et $(q+1)b > a$ car $q+1 \notin \mathcal{N}$ donc

$$qb \leqslant a < (q+1)b = qb + b.$$

On définit alors $r = a - qb$, r vérifie alors $0 \leqslant r = a - qb < b$.
Unicité. Supposons que q', r' soient deux entiers qui vérifient les conditions du théorème. Tout d'abord $a = bq + r = bq' + r'$ et donc $b(q - q') = r' - r$. D'autre part $0 \leqslant r' < b$ et $0 \leqslant r < b$ donc $-b < r' - r < b$ (notez au passage la manipulation des inégalités). Mais $r' - r = b(q - q')$ donc on obtient $-b < b(q - q') < b$. On peut diviser par $b > 0$ pour avoir $-1 < q - q' < 1$. Comme $q - q'$ est un entier, la seule possibilité est $q - q' = 0$ et donc $q = q'$. Repartant de $r' - r = b(q - q')$ on obtient maintenant $r = r'$.

1.2. pgcd de deux entiers

Définition 14

Soient $a, b \in \mathbb{Z}$ deux entiers, non tous les deux nuls. Le plus grand entier qui divise à la fois a et b s'appelle le ***plus grand diviseur commun*** de a, b et se note $\text{pgcd}(a, b)$.

Exemple 25

- $\text{pgcd}(21, 14) = 7$, $\text{pgcd}(12, 32) = 4$, $\text{pgcd}(21, 26) = 1$.
- $\text{pgcd}(a, ka) = a$, pour tout $k \in \mathbb{Z}$ et $a \geqslant 0$.
- Cas particuliers. Pour tout $a \geqslant 0$: $\text{pgcd}(a, 0) = a$ et $\text{pgcd}(a, 1) = 1$.

1.3. Algorithme d'Euclide

Lemme 1

Soient $a, b \in \mathbb{N}^*$. Écrivons la division euclidienne $a = bq + r$. Alors

$$\text{pgcd}(a, b) = \text{pgcd}(b, r)$$

En fait on a même $\text{pgcd}(a, b) = \text{pgcd}(b, a - qb)$ pour tout $q \in \mathbb{Z}$. Mais pour optimiser l'algorithme d'Euclide on applique le lemme avec q le quotient.

Démonstration

Nous allons montrer que les diviseurs de a et de b sont exactement les mêmes que les diviseurs de b et r. Cela impliquera le résultat car les plus grands diviseurs seront bien sûr les mêmes.

- Soit d un diviseur de a et de b. Alors d divise b donc aussi bq, en plus d divise a donc d divise $bq - a = r$.
- Soit d un diviseur de b et de r. Alors d divise aussi $bq + r = a$.

Algorithme d'Euclide.

On souhaite calculer le pgcd de $a, b \in \mathbb{N}^*$. On peut supposer $a \geqslant b$. On calcule des divisions euclidiennes successives. Le pgcd sera le dernier reste non nul.

- division de a par b, $a = bq_1 + r_1$. Par le lemme 1, $\text{pgcd}(a, b) = \text{pgcd}(b, r_1)$ et si $r_1 = 0$ alors $\text{pgcd}(a, b) = b$ sinon on continue :
- $b = r_1 q_2 + r_2$, $\quad \text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2)$,
- $r_1 = r_2 q_3 + r_3$, $\quad \text{pgcd}(a, b) = \text{pgcd}(r_2, r_3)$,
- ...
- $r_{k-2} = r_{k-1} q_k + r_k$, $\text{pgcd}(a, b) = \text{pgcd}(r_{k-1}, r_k)$,
- $r_{k-1} = r_k q_k + 0$. $\text{pgcd}(a, b) = \text{pgcd}(r_k, 0) = r_k$.

Comme à chaque étape le reste est plus petit que le quotient on sait que $0 \leqslant r_{i+1} < r_i$. Ainsi l'algorithme se termine car nous sommes sûr d'obtenir un reste nul, les restes formant une suite décroissante d'entiers positifs ou nuls : $b > r_1 > r_2 > \ldots \geqslant 0$

Exemple 26

Calculons le pgcd de $a = 600$ et $b = 124$.

$$\begin{array}{rcrcrcr} 600 & = & 124 & \times & 4 & + & 104 \\ 124 & = & 104 & \times & 1 & + & 20 \\ 104 & = & 20 & \times & 5 & + & 4 \\ 20 & = & 4 & \times & 5 & + & 0 \end{array}$$

Ainsi $\text{pgcd}(600,124) = 4$.

Voici un exemple plus compliqué :

Exemple 27

Calculons $\text{pgcd}(9945,3003)$.

$$\begin{array}{rcrcrcr} 9945 & = & 3003 & \times & 3 & + & 936 \\ 3003 & = & 936 & \times & 3 & + & 195 \\ 936 & = & 195 & \times & 4 & + & 156 \\ 195 & = & 156 & \times & 1 & + & 39 \\ 156 & = & 39 & \times & 4 & + & 0 \end{array}$$

Ainsi $\text{pgcd}(9945,3003) = 39$.

1.4. Nombres premiers entre eux

Définition 15

Deux entiers a,b sont ***premiers entre eux*** si $\text{pgcd}(a,b) = 1$.

Exemple 28

Pour tout $a \in \mathbb{Z}$, a et $a+1$ sont premiers entre eux. En effet soit d un diviseur commun à a et à $a+1$. Alors d divise aussi $a+1-a$. Donc d divise 1 mais alors $d = -1$ ou $d = +1$. Le plus grand diviseur de a et $a+1$ est donc 1. Et donc $\text{pgcd}(a,a+1) = 1$.

Si deux entiers ne sont pas premiers entre eux, on peut s'y ramener en divisant par leur pgcd :

Exemple 29

Pour deux entiers quelconques $a,b \in \mathbb{Z}$, notons $d = \text{pgcd}(a,b)$. La décomposition suivante est souvent utile :

$$\begin{cases} a = a'd \\ b = b'd \end{cases} \quad \text{avec} \quad a',b' \in \mathbb{Z} \text{ et } \text{pgcd}(a',b') = 1$$

Mini-exercices

1. Écrire la division euclidienne de 111 111 par $20xx$, où $20xx$ est l'année en cours.
2. Montrer qu'un diviseur positif de 10 008 et de 10 014 appartient nécessairement à $\{1,2,3,6\}$.

3. Calculer pgcd(560, 133), pgcd(12121, 789), pgcd(99999, 1110).
4. Trouver tous les entiers $1 \leqslant a \leqslant 50$ tels que a et 50 soient premiers entre eux. Même question avec 52.

2. Théorème de Bézout

2.1. Théorème de Bézout

Théorème 4. Théorème de Bézout

Soient a, b des entiers. Il existe des entiers $u, v \in \mathbb{Z}$ tels que

$$au + bv = \text{pgcd}(a, b)$$

La preuve découle de l'algorithme d'Euclide. Les entiers u, v ne sont pas uniques. Les entiers u, v sont des ***coefficients de Bézout***. Ils s'obtiennent en «remontant» l'algorithme d'Euclide.

Exemple 30

Calculons les coefficients de Bézout pour $a = 600$ et $b = 124$. Nous reprenons les calculs effectués pour trouver $\text{pgcd}(600, 124) = 4$. La partie gauche est l'algorithme d'Euclide. La partie droite s'obtient de *bas en haut*. On exprime le pgcd à l'aide de la dernière ligne où le reste est non nul. Puis on remplace le reste de la ligne précédente, et ainsi de suite jusqu'à arriver à la première ligne.

$$\begin{array}{rclcccl}
600 & = & 124 & \times & 4 & + & 104 \\
124 & = & 104 & \times & 1 & + & 20 \\
104 & = & 20 & \times & 5 & + & 4 \\
20 & = & 4 & \times & 5 & + & 0
\end{array}
\qquad
\begin{array}{rcl}
4 & = & 124 \times (-5) + (600 - 124 \times 4) \times 6 = 600 \times 6 + 124 \times (-29) \\
4 & = & 104 - (124 - 104 \times 1) \times 5 = 124 \times (-5) + 104 \times 6 \\
4 & = & 104 - 20 \times 5
\end{array}$$

Ainsi pour $u = 6$ et $v = -29$ alors $600 \times 6 + 124 \times (-29) = 4$.

Remarque

- Soignez vos calculs et leur présentation. C'est un algorithme : vous devez aboutir au bon résultat ! Dans la partie droite, il faut à chaque ligne bien la reformater. Par exemple $104 - (124 - 104 \times 1) \times 5$ se réécrit en $124 \times (-5) + 104 \times 6$ afin de pouvoir remplacer ensuite 104.
- N'oubliez de vérifier vos calculs ! C'est rapide et vous serez certain que vos calculs sont exacts. Ici on vérifie à la fin que $600 \times 6 + 124 \times (-29) = 4$.

Exemple 31

Calculons les coefficients de Bézout correspondant à $\text{pgcd}(9945, 3003) = 39$.

$$\begin{array}{rclcccl}
9945 & = & 3003 & \times & 3 & + & 936 \\
3003 & = & 936 & \times & 3 & + & 195 \\
936 & = & 195 & \times & 4 & + & 156 \\
195 & = & 156 & \times & 1 & + & 39 \\
156 & = & 39 & \times & 4 & + & 0
\end{array}
\qquad
\begin{array}{rcl}
39 & = & 9945 \times (-16) + 3003 \times 53 \\
39 & = & \cdots \\
39 & = & \cdots \\
39 & = & 195 - 156 \times 1
\end{array}$$

À vous de finir les calculs. On obtient $9945 \times (-16) + 3003 \times 53 = 39$.

2.2. Corollaires du théorème de Bézout

Corollaire 2

Si $d|a$ et $d|b$ alors $d|\operatorname{pgcd}(a,b)$.

Exemple : $4|16$ et $4|24$ donc 4 doit divisé $\operatorname{pgcd}(16,24)$ qui effectivement vaut 8.

Démonstration

Comme $d|au$ et $d|bv$ donc $d|au+bv$. Par le théorème de Bézout $d|\operatorname{pgcd}(a,b)$.

Corollaire 3

Soient a,b deux entiers. a,b sont premiers entre eux **si et seulement si** il existe $u,v \in \mathbb{Z}$ tels que

$$\boxed{au + bv = 1}$$

Démonstration

Le sens $\Rightarrow$ est une conséquence du théorème de Bézout.
Pour le sens $\Leftarrow$ on suppose qu'il existe u,v tels que $au+bv=1$. Comme $\operatorname{pgcd}(a,b)|a$ alors $\operatorname{pgcd}(a,b)|au$. De même $\operatorname{pgcd}(a,b)|bv$. Donc $\operatorname{pgcd}(a,b)|au+bv=1$. Donc $\operatorname{pgcd}(a,b)=1$.

Remarque

Si on trouve deux entiers u',v' tels que $au'+bv'=d$, cela n'implique **pas** que $d=\operatorname{pgcd}(a,b)$. On sait seulement alors que $\operatorname{pgcd}(a,b)|d$. Par exemple $a=12$, $b=8$; $12\times 1+8\times 3=36$ et $\operatorname{pgcd}(a,b)=4$.

Corollaire 4. Lemme de Gauss

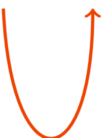
Soient $a,b,c \in \mathbb{Z}$.

$$\boxed{\text{Si} \quad a|bc \quad \text{et} \quad \operatorname{pgcd}(a,b)=1 \quad \text{alors} \quad a|c}$$

Exemple : si $4|7\times c$, et comme 4 et 7 sont premiers entre eux, alors $4|c$.

Démonstration

Comme $\operatorname{pgcd}(a,b)=1$ alors il existe $u,v \in \mathbb{Z}$ tels que $au+bv=1$. On multiplie cette égalité par c pour obtenir $acu+bcv=c$. Mais $a|acu$ et par hypothèse $a|bcv$ donc a divise $acu+bcv=c$.



2.3. Équations $ax+by=c$

Proposition 21

Considérons l'équation

$$ax + by = c \qquad \text{(E)}$$

où $a, b, c \in \mathbb{Z}$.

1. L'équation (E) possède des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $\operatorname{pgcd}(a, b)|c$.
2. Si $\operatorname{pgcd}(a, b)|c$ alors il existe même une infinité de solutions entières et elles sont exactement les $(x, y) = (x_0 + \alpha k, y_0 + \beta k)$ avec $x_0, y_0, \alpha, \beta \in \mathbb{Z}$ fixés et k parcourant $\mathbb{Z}$.

Le premier point est une conséquence du théorème de Bézout. Nous allons voir sur un exemple comment prouver le second point et calculer explicitement les solutions. Il est bon de refaire toutes les étapes de la démonstration à chaque fois.

Exemple 32

Trouver les solutions entières de

$$161x + 368y = 115 \qquad \text{(E)}$$

– **Première étape. Y a-t'il de solutions ? L'algorithme d'Euclide.** On effectue l'algorithme d'Euclide pour calculer le pgcd de $a = 161$ et $b = 368$.

$$\begin{array}{rclcccl} 368 & = & 161 & \times & 2 & + & 46 \\ 161 & = & 46 & \times & 3 & + & 23 \\ 46 & = & 23 & \times & 2 & + & 0 \end{array}$$

Donc $\operatorname{pgcd}(368, 161) = 23$. Comme $115 = 5 \times 23$ alors $\operatorname{pgcd}(368, 161)|115$. Par le théorème de Bézout, l'équation (E) admet des solutions entières.

– **Deuxième étape. Trouver une solution particulière : la remontée de l'algorithme d'Euclide.** On effectue la remontée de l'algorithme d'Euclide pour calculer les coefficients de Bézout.

$$\begin{array}{rclcccl} 368 & = & 161 & \times & 2 & + & 46 \\ 161 & = & 46 & \times & 3 & + & 23 \\ 46 & = & 23 & \times & 2 & + & 0 \end{array} \qquad \begin{array}{rcl} 23 & = & 161 + (368 - 2 \times 161) \times (-3) = 161 \times 7 + 368 \times (-3) \\ 23 & = & 161 - 3 \times 46 \end{array}$$

On trouve donc $161 \times 7 + 368 \times (-3) = 23$. Comme $115 = 5 \times 23$ en multipliant par 5 on obtient :

$$161 \times 35 + 368 \times (-15) = 115$$

Ainsi $(x_0, y_0) = (35, -15)$ est une ***solution particulière*** de (E).

– **Troisième étape. Recherche de toutes les solutions.** Soit $(x, y) \in \mathbb{Z}^2$ une solution de (E). Nous savons que (x_0, y_0) est aussi solution. Ainsi :

$$161x + 368y = 115 \quad \text{et} \quad 161x_0 + 368y_0 = 115$$

(on n'a aucun intérêt à remplacer x_0 et y_0 par leurs valeurs). La différence de ces deux

égalités conduit à

$$\begin{aligned} & 161 \times (x - x_0) + 368 \times (y - y_0) = 0 \\ \Longrightarrow\ & 23 \times 7 \times (x - x_0) + 23 \times 16 \times (y - y_0) = 0 \\ \Longrightarrow\ & 7(x - x_0) = -16(y - y_0) \qquad (*) \end{aligned}$$

Nous avons simplifier par 23 qui est le pgcd de 161 et 368. (Attention, n'oubliez surtout pas cette simplification, sinon la suite du raisonnement serait fausse.)
Ainsi $7|16(y - y_0)$, or $\text{pgcd}(7, 16) = 1$ donc par le lemme de Gauss $7|y - y_0$. Il existe donc $k \in \mathbb{Z}$ tel que $y - y_0 = 7 \times k$. Repartant de l'équation $(*)$: $7(x - x_0) = -16(y - y_0)$. On obtient maintenant $7(x - x_0) = -16 \times 7 \times k$. D'où $x - x_0 = -16k$. (C'est le même k pour x et pour y.) Nous avons donc $(x, y) = (x_0 - 16k, y_0 + 7k)$. Il n'est pas dur de voir que tout couple de cette forme est solution de l'équation (E). Il reste donc juste à substituer (x_0, y_0) par sa valeur et nous obtenons :

Les solutions entières de $161x + 368y = 115$ sont les $(x, y) = (35 - 16k, -15 + 7k)$, k parcourant $\mathbb{Z}$.

Pour se rassurer, prenez une valeur de k au hasard et vérifiez que vous obtenez bien une solution de l'équation.

2.4. ppcm

Définition 16

Le $\text{ppcm}(a, b)$ (***plus petit multiple commun***) est le plus petit entier $\geqslant 0$ divisible par a et par b.

Par exemple $\text{ppcm}(12, 9) = 36$.
Le pgcd et le ppcm sont liés par la formule suivante :

Proposition 22

Si a, b sont des entiers (non tous les deux nuls) alors

$$\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |ab|$$

Démonstration

Posons $d = \text{pgcd}(a, b)$ et $m = \frac{|ab|}{\text{pgcd}(a,b)}$. Pour simplifier on suppose $a > 0$ et $b > 0$. On écrit $a = da'$ et $b = db'$. Alors $ab = d^2a'b'$ et donc $m = da'b'$. Ainsi $m = ab' = a'b$ est un multiple de a et de b.
Il reste à montrer que c'est le plus petit multiple. Si n est un autre multiple de a et de b alors $n = ka = \ell b$ donc $kda' = \ell db'$ et $ka' = \ell b'$. Or $\text{pgcd}(a', b') = 1$ et $a'|\ell b'$ donc $a'|\ell$. Donc $a'b|\ell b$ et ainsi $m = a'b|\ell b = n$.

Voici un autre résultat concernant le ppcm qui se démontre en utilisant la décomposition en facteurs premiers :

Proposition 23

Si $a|c$ et $b|c$ alors $\text{ppcm}(a,b)|c$.

Il serait faux de penser que $ab|c$. Par exemple $6|36$, $9|36$ mais 6×9 ne divise pas 36. Par contre $\text{ppcm}(6,9) = 18$ divise bien 36.

Mini-exercices

1. Calculer les coefficients de Bézout correspondant à $\text{pgcd}(560,133)$, $\text{pgcd}(12\,121,789)$.
2. Montrer à l'aide d'un corollaire du théorème de Bézout que $\text{pgcd}(a,a+1) = 1$.
3. Résoudre les équations : $407x + 129y = 1$; $720x + 54y = 6$; $216x + 92y = 8$.
4. Trouver les couples (a,b) vérifiant $\text{pgcd}(a,b) = 12$ et $\text{ppcm}(a,b) = 360$.

3. Nombres premiers

Les nombres premiers sont –en quelque sorte– les briques élémentaires des entiers : tout entier s'écrit comme produit de nombres premiers.

3.1. Une infinité de nombres premiers

Définition 17

Un ***nombre premier*** p est un entier $\geqslant 2$ dont les seuls diviseurs positifs sont 1 et p.

Exemples : $2,3,5,7,11$ sont premiers, $4 = 2 \times 2$, $6 = 2 \times 3$, $8 = 2 \times 4$ ne sont pas premiers.

Lemme 2

Tout entier $n \geqslant 2$ admet un diviseur qui est un nombre premier.

Démonstration

Soit $\mathcal{D}$ l'ensemble des diviseurs de n qui sont $\geqslant 2$:

$$\mathcal{D} = \{k \geqslant 2 \mid k|n\}.$$

L'ensemble $\mathcal{D}$ est non vide (car $n \in \mathcal{D}$), notons alors $p = \min \mathcal{D}$.
Supposons, par l'absurde, que p ne soit pas un nombre premier alors p admet un diviseur q tel que $1 < q < p$ mais alors q est aussi un diviseur de n et donc $q \in \mathcal{D}$ avec $q < p$. Ce qui donne une contradiction car p est le minimum. Conclusion : p est un nombre premier. Et comme $p \in \mathcal{D}$, p divise n.

Proposition 24

Il existe une infinité de nombres premiers.

Démonstration

Par l'absurde, supposons qu'il n'y ait qu'un nombre fini de nombres premiers que l'on note $p_1 = 2$, $p_2 = 3$, p_3,..., p_n. Considérons l'entier $N = p_1 \times p_2 \times \cdots \times p_n + 1$. Soit p un diviseur premier de N (un tel p existe par le lemme précédent), alors d'une part p est l'un des entiers p_i donc $p | p_1 \times \cdots \times p_n$, d'autre part $p|N$ donc p divise la différence $N - p_1 \times \cdots \times p_n = 1$. Cela implique que $p = 1$, ce qui contredit que p soit un nombre premier.
Cette contradiction nous permet de conclure qu'il existe une infinité de nombres premiers.

3.2. Eratosthène et Euclide

Comment trouver les nombres premiers ? Le ***crible d'Eratosthène*** permet de trouver les premiers nombres premiers. Pour cela on écrit les premiers entiers : pour notre exemple de 2 à 25.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Rappelons-nous qu'un diviseur positif d'un entier n est inférieur ou égal à n. Donc 2 ne peut avoir comme diviseurs que 1 et 2 et est donc premier. On entoure 2. Ensuite on raye (ici en grisé) tous les multiples suivants de 2 qui ne seront donc pas premiers (car divisible par 2) :

[2] 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Le premier nombre restant de la liste est 3 et est nécessairement premier : il n'est pas divisible par un diviseur plus petit (sinon il serait rayé). On entoure 3 et on raye tous les multiples de 3 (6, 9, 12, ...).

[2] [3] 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Le premier nombre restant est 5 et est donc premier. On raye les multiples de 5.

[2] [3] 4 [5] 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

7 est donc premier, on raye les multiples de 7 (ici pas de nouveaux nombres à barrer). Ainsi de suite : $11, 13, 17, 19, 23$ sont premiers.

[2] [3] 4 [5] 6 [7] 8 9 10 [11] 12 [13] 14 15 16 [17] 18 [19] 20 21 22 [23] 24 25

Remarque

Si un nombre n n'est pas premier alors un de ses facteurs est $\leqslant \sqrt{n}$. En effet si $n = a \times b$ avec $a, b \geqslant 2$ alors $a \leqslant \sqrt{n}$ ou $b \leqslant \sqrt{n}$ (réfléchissez par l'absurde !). Par exemple pour tester si un nombre $\leqslant 100$ est premier il suffit de tester les diviseurs $\leqslant 10$. Et comme il suffit de tester les diviseurs premiers, il suffit en fait de tester la divisibilité par $2, 3, 5$ et 7. Exemple : 89 n'est pas divisible par $2, 3, 5, 7$ et est donc un nombre premier.

Proposition 25. Lemme d'Euclide

Soit p un nombre premier. Si $p|ab$ alors $p|a$ ou $p|b$.

Démonstration

Si p ne divise pas a alors p et a sont premiers entre eux (en effet les diviseurs de p sont 1 et p, mais seul 1 divise aussi a, donc $\mathrm{pgcd}(a,p)=1$). Ainsi par le lemme de Gauss $p|b$.

Exemple 33

Si p est un nombre premier, $\sqrt{p}$ n'est pas un nombre rationnel.
La preuve se fait par l'absurde : écrivons $\sqrt{p}=\frac{a}{b}$ avec $a\in\mathbb{Z}, b\in\mathbb{N}^*$ et $\mathrm{pgcd}(a,b)=1$. Alors $p=\frac{a^2}{b^2}$ donc $pb^2=a^2$. Ainsi $p|a^2$ donc par le lemme d'Euclide $p|a$. On peut alors écrire $a=pa'$ avec a' un entier. De l'équation $pb^2=a^2$ on tire alors $b^2=pa'^2$. Ainsi $p|b^2$ et donc $p|b$. Maintenant $p|a$ et $p|b$ donc a et b ne sont pas premiers entre eux. Ce qui contredit $\mathrm{pgcd}(a,b)=1$. Conclusion $\sqrt{p}$ n'est pas rationnel.

3.3. Décomposition en facteurs premiers

Théorème 5

Soit $n\geqslant 2$ un entier. Il existe des nombres premiers $p_1<p_2<\ldots<p_r$ et des exposants entiers $\alpha_1,\alpha_2,\ldots,\alpha_r\geqslant 1$ tels que :

$$n=p_1^{\alpha_1}\times p_2^{\alpha_2}\times\cdots\times p_r^{\alpha_r}.$$

De plus les p_i et les α_i $(i=1,\ldots,r)$ sont uniques.

Exemple : $24=2^3\times 3$ est la décomposition en facteurs premiers. Par contre $36=2^2\times 9$ n'est pas la décomposition en facteurs premiers c'est $2^2\times 3^2$.

Remarque

La principale raison pour laquelle on choisit de dire que 1 n'est pas un nombre premier, c'est que sinon il n'y aurait plus unicité de la décomposition : $24=2^3\times 3=1\times 2^3\times 3=1^2\times 2^3\times 3=\cdots$

Démonstration

Existence. Nous allons démontrer l'existence de la décomposition par une récurrence sur n.
L'entier $n=2$ est déjà décomposé. Soit $n\geqslant 3$, supposons que tout entier $<n$ admette une décomposition en facteurs premiers. Notons p_1 le plus petit nombre premier divisant n (voir le lemme 2). Si n est un nombre premier alors $n=p_1$ et c'est fini. Sinon on définit l'entier $n'=\frac{n}{p_1}<n$ et on applique notre hypothèse de récurrence à n' qui admet une décomposition en facteurs premiers. Alors $n=p_1\times n'$ admet aussi une décomposition.

Unicité. Nous allons démontrer qu'une telle décomposition est unique en effectuant cette fois une récurrence sur la somme des exposants $\sigma=\sum_{i=1}^{r}\alpha_i$.
Si $\sigma=1$ cela signifie $n=p_1$ qui est bien l'unique écriture possible.
Soit $\sigma\geqslant 2$. On suppose que les entiers dont la somme des exposants est $<\sigma$ ont une unique décomposition. Soit n un entier dont la somme des exposants vaut σ. Écrivons le avec deux décompositions :

$$n=p_1^{\alpha_1}\times p_2^{\alpha_2}\times\cdots\times p_r^{\alpha_r}=q_1^{\beta_1}\times q_2^{\beta_2}\times\cdots\times q_s^{\beta_s}.$$

(On a $p_1 < p_2 < \cdots$ et $q_1 < q_2 < \cdots$.)
Si $p_1 < q_1$ alors $p_1 < q_j$ pour tous les $j = 1,\ldots,s$. Ainsi p_1 divise $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r} = n$ mais ne divise pas $q_1^{\beta_1} \times q_2^{\beta_2} \times \cdots \times q_s^{\beta_s} = n$. Ce qui est absurde. Donc $p_1 \geqslant q_1$.
Si $p_1 > q_1$ un même raisonnement conduit aussi à une contradiction. On conclut que $p_1 = q_1$. On pose alors

$$n' = \frac{n}{p_1} = p_1^{\alpha_1 - 1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r} = q_1^{\beta_1 - 1} \times q_2^{\beta_2} \times \cdots \times q_s^{\beta_s}$$

L'hypothèse de récurrence qui s'applique à n' implique que ces deux décompositions sont les mêmes. Ainsi $r = s$ et $p_i = q_i$, $\alpha_i = \beta_i$, $i = 1,\ldots,r$.

Exemple 34

$$504 = 2^3 \times 3^2 \times 7, \quad 300 = 2^2 \times 3 \times 5^2.$$

Pour calculer le pgcd on réécrit ces décompositions :

$$504 = 2^3 \times 3^2 \times 5^0 \times 7^1, \quad 300 = 2^2 \times 3^1 \times 5^2 \times 7^0.$$

Le pgcd est le nombre obtenu en prenant le plus petit exposant de chaque facteur premier :

$$\text{pgcd}(504, 300) = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12.$$

Pour le ppcm on prend le plus grand exposant de chaque facteur premier :

$$\text{ppcm}(504, 300) = 2^3 \times 3^2 \times 5^2 \times 7^1 = 12\,600$$

Mini-exercices

1. Montrer que $n! + 1$ n'est divisible par aucun des entiers $2, 3, \ldots, n$. Est-ce toujours un nombre premier ?
2. Trouver tous les nombres premiers $\leqslant 103$.
3. Décomposer $a = 2\,340$ et $b = 15\,288$ en facteurs premiers. Calculer leur pgcd et leur ppcm.
4. Décomposer $48\,400$ en produit de facteurs premiers. Combien $48\,400$ admet-il de diviseurs ?
5. Soient $a, b \geqslant 0$. À l'aide de la décomposition en facteurs premiers, reprouver la formule $\text{pgcd}(a,b) \times \text{ppcm}(a,b) = a \times b$.

4. Congruences

4.1. Définition

Définition 18

Soit $n \geqslant 2$ un entier. On dit que a est ***congru*** à b ***modulo*** n, si n divise $b-a$. On note alors

$$a \equiv b \pmod{n}.$$

On note aussi parfois $a = b \pmod{n}$ ou $a \equiv b[n]$. Une autre formulation est

$$\boxed{a \equiv b \pmod{n} \iff \exists k \in \mathbb{Z} \quad a = b + kn.}$$

Remarquez que n divise a si et seulement si $a \equiv 0 \pmod{n}$.

Proposition 26

1. La relation «congru modulo n» est une relation d'équivalence :
   - $a \equiv a \pmod{n}$,
   - si $a \equiv b \pmod{n}$ alors $b \equiv a \pmod{n}$,
   - si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ alors $a \equiv c \pmod{n}$.
2. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $a + c \equiv b + d \pmod{n}$.
3. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $a \times c \equiv b \times d \pmod{n}$.
4. Si $a \equiv b \pmod{n}$ alors pour tout $k \geqslant 0$, $a^k \equiv b^k \pmod{n}$.

Exemple 35

- $15 \equiv 1 \pmod{7}$, $72 \equiv 2 \pmod{7}$, $3 \equiv -11 \pmod{7}$,
- $5x + 8 \equiv 3 \pmod{5}$ pour tout $x \in \mathbb{Z}$,
- $11^{20xx} \equiv 1^{20xx} \equiv 1 \pmod{10}$, où $20xx$ est l'année en cours.

Démonstration

1. Utiliser la définition.
2. Idem.
3. Prouvons la propriété multiplicative : $a \equiv b \pmod{n}$ donc il existe $k \in \mathbb{Z}$ tel que $a = b + kn$ et $c \equiv d \pmod{n}$ donc il existe $\ell \in \mathbb{Z}$ tel que $c \equiv d + \ell n$. Alors $a \times c = (b + kn) \times (d + \ell n) = bd + (b\ell + dk + k\ell n)n$ qui est bien de la forme $bd + mn$ avec $m \in \mathbb{Z}$. Ainsi $ac \equiv bd \pmod{n}$.
4. C'est une conséquence du point précédent : avec $a = c$ et $b = d$ on obtient $a^2 \equiv b^2 \pmod{n}$. On continue par récurrence.

Exemple 36

Critère de divisibilité par 9.

$\boxed{N \text{ est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.}}$

Pour prouver cela nous utilisons les congruences. Remarquons d'abord que $9|N$ équivaut à $N \equiv 0 \pmod{9}$ et notons aussi que $10 \equiv 1 \pmod{9}$, $10^2 \equiv 1 \pmod{9}$, $10^3 \equiv 1 \pmod{9}$,...
Nous allons donc calculer N modulo 9. Écrivons N en base 10 : $N = \overline{a_k \cdots a_2 a_1 a_0}$ (a_0 est le

chiffre des unités, a_1 celui des dizaines,...) alors $N = 10^k a_k + \cdots + 10^2 a_2 + 10^1 a_1 + a_0$. Donc

$$\begin{aligned} N &= 10^k a_k + \cdots + 10^2 a_2 + 10^1 a_1 + a_0 \\ &\equiv a_k + \cdots + a_2 + a_1 + a_0 \pmod 9 \end{aligned}$$

Donc N est congru à la somme de ses chiffres modulo 9. Ainsi $N \equiv 0 \pmod 9$ si et seulement si la somme des chiffres vaut 0 modulo 9.
Voyons cela sur un exemple : $N = 488\,889$. Ici $a_0 = 9$ est le chiffre des unités, $a_1 = 8$ celui des dizaines,... Cette écriture décimale signifie $N = 4 \cdot 10^5 + 8 \cdot 10^4 + 8 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10 + 9$.

$$\begin{aligned} N &= 4 \cdot 10^5 + 8 \cdot 10^4 + 8 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10 + 9 \\ &\equiv 4 + 8 + 8 + 8 + 8 + 9 \pmod 9 \\ &\equiv 45 \pmod 9 \qquad \text{et on refait la somme des chiffres de 45} \\ &\equiv 9 \pmod 9 \\ &\equiv 0 \pmod 9 \end{aligned}$$

Ainsi nous savons que $488\,889$ est divisible par 9 sans avoir effectué de division euclidienne.

Remarque

Pour trouver un «bon» représentant de $a \pmod n$ on peut aussi faire la division euclidienne de a par n : $a = bn + r$ alors $a \equiv r \pmod n$ et $0 \leqslant r < n$.

Exemple 37

Les calculs bien menés avec les congruences sont souvent très rapides. Par exemple on souhaite calculer $2^{21} \pmod{37}$ (plus exactement on souhaite trouver $0 \leqslant r < 37$ tel que $2^{21} \equiv r \pmod{37}$). Plusieurs méthodes :

1. On calcule 2^{21}, puis on fait la division euclidienne de 2^{21} par 37, le reste est notre résultat. C'est laborieux !
2. On calcule successivement les 2^k modulo 37 : $2^1 \equiv 2 \pmod{37}$, $2^2 \equiv 4 \pmod{37}$, $2^3 \equiv 8 \pmod{37}$, $2^4 \equiv 16 \pmod{37}$, $2^5 \equiv 32 \pmod{37}$. Ensuite on n'oublie pas d'utiliser les congruences : $2^6 \equiv 64 \equiv 27 \pmod{37}$. $2^7 \equiv 2 \cdot 2^6 \equiv 2 \cdot 27 \equiv 54 \equiv 17 \pmod{37}$ et ainsi de suite en utilisant le calcul précédent à chaque étape. C'est assez efficace et on peut raffiner : par exemple on trouve $2^8 \equiv 34 \pmod{37}$ mais donc aussi $2^8 \equiv -3 \pmod{37}$ et donc $2^9 \equiv 2 \cdot 2^8 \equiv 2 \cdot (-3) \equiv -6 \equiv 31 \pmod{37}$,...
3. Il existe une méthode encore plus efficace : on écrit l'exposant 21 en base 2 : $21 = 2^4 + 2^2 + 2^0 = 16 + 4 + 1$. Alors $2^{21} = 2^{16} \cdot 2^4 \cdot 2^1$. Et il est facile de calculer successivement chacun de ces termes car les exposants sont des puissances de 2. Ainsi $2^8 \equiv (2^4)^2 \equiv 16^2 \equiv 256 \equiv 34 \equiv -3 \pmod{37}$ et $2^{16} \equiv \left(2^8\right)^2 \equiv (-3)^2 \equiv 9 \pmod{37}$. Nous obtenons $2^{21} \equiv 2^{16} \cdot 2^4 \cdot 2^1 \equiv 9 \times 16 \times 2 \equiv 288 \equiv 29 \pmod{37}$.

4.2. Équation de congruence $ax \equiv b \pmod n$

Proposition 27

Soit $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$ fixés et $n \geqslant 2$. Considérons l'équation $\boxed{ax \equiv b \pmod n}$ d'inconnue $x \in \mathbb{Z}$:

1. Il existe des solutions si et seulement si $\operatorname{pgcd}(a,n)|b$.
2. Les solutions sont de la forme $x = x_0 + \ell \frac{n}{\operatorname{pgcd}(a,n)}$, $\ell \in \mathbb{Z}$ où x_0 est une solution particulière. Il existe donc $\operatorname{pgcd}(a,n)$ classes de solutions.

Exemple 38

Résolvons l'équation $9x \equiv 6 \pmod{24}$. Comme $\operatorname{pgcd}(9,24) = 3$ divise 6 la proposition ci-dessus nous affirme qu'il existe des solutions. Nous allons les calculer. (Il est toujours préférable de refaire rapidement les calculs que d'apprendre la formule). Trouver x tel que $9x \equiv 6 \pmod{24}$ est équivalent à trouver x et k tels que $9x = 6+24k$. Mis sous la forme $9x-24k = 6$ il s'agit alors d'une équation que nous avons étudier en détails (voir section 2.3). Il y a bien des solutions car $\operatorname{pgcd}(9,24) = 3$ divise 6. En divisant par le pgcd on obtient l'équation équivalente :

$$3x - 8k = 2.$$

Pour le calcul du pgcd et d'une solution particulière nous utilisons normalement l'algorithme d'Euclide et sa remontée. Ici il est facile de trouver une solution particulière ($x_0 = 6, k_0 = 2$) à la main.

On termine comme pour les équations de la section 2.3. Si (x,k) est une solution de $3x-8k = 2$ alors par soustraction on obtient $3(x-x_0)-8(k-k_0) = 0$ et on trouve $x = x_0 +8\ell$, avec $\ell \in \mathbb{Z}$ (le terme k ne nous intéresse pas). Nous avons donc trouvé les x qui sont solutions de $3x-8k = 2$, ce qui équivaut à $9x-24k = 6$, ce qui équivaut encore à $9x \equiv 6 \pmod{24}$. Les solutions sont de la forme $x = 6+8\ell$. On préfère les regrouper en 3 classes modulo 24 :

$$x_1 = 6+24m, \quad x_2 = 14+24m, \quad x_3 = 22+24m \qquad \text{avec } m \in \mathbb{Z}.$$

Remarque

Expliquons le terme de «classe» utilisé ici. Nous avons considérer ici que l'équation $9x \equiv 6 \pmod{24}$ est une équation d'entiers. On peut aussi considérer que $9, x, 6$ sont des classes d'équivalence modulo 24, et l'on noterait alors $\overline{9}\overline{x} = \overline{6}$. On trouverait comme solutions trois classes d'équivalence :

$$\overline{x_1} = \overline{6}, \quad \overline{x_2} = \overline{14}, \quad \overline{x_3} = \overline{22}.$$

Démonstration

1.
$$\begin{aligned} & x \in \mathbb{Z} \text{ est un solution de l'équation } ax \equiv b \pmod n \\ \iff & \exists k \in \mathbb{Z} \quad ax = b+kn \\ \iff & \exists k \in \mathbb{Z} \quad ax-kn = b \\ \iff & \operatorname{pgcd}(a,n)|b \quad \text{par la proposition 21} \end{aligned}$$

Nous avons juste transformé notre équation $ax \equiv b \pmod n$ en une équation $ax-kn = b$ étudiée auparavant (voir section 2.3), seules les notations changent : $au+bv = c$ devient $ax-kn = b$.

2. Supposons qu'il existe des solutions. Nous allons noter $d = \text{pgcd}(a,n)$ et écrire $a = da'$, $n = dn'$ et $b = db'$ (car par le premier point $d|b$). L'équation $ax - kn = b$ d'inconnues $x, k \in \mathbb{Z}$ est alors équivalente à l'équation $a'x - kn' = b'$, notée ($\star$). Nous savons résoudre cette équation (voir de nouveau la proposition 21), si (x_0, k_0) est une solution particulière de ($\star$) alors on connaît tous les (x,k) solutions. En particulier $x = x_0 + \ell n'$ avec $\ell \in \mathbb{Z}$ (les k ne nous intéressent pas ici).

   Ainsi les solutions $x \in \mathbb{Z}$ sont de la forme $x = x_0 + \ell \frac{n}{\text{pgcd}(a,n)}$, $\ell \in \mathbb{Z}$ où x_0 est une solution particulière de $ax \equiv b \pmod n$. Et modulo n cela donne bien $\text{pgcd}(a,n)$ classes distinctes.

4.3. Petit théorème de Fermat

Théorème 6. Petit théorème de Fermat

Si p est un nombre premier et $a \in \mathbb{Z}$ alors

$$\boxed{a^p \equiv a \pmod p}$$

Corollaire 5

Si p ne divise pas a alors

$$\boxed{a^{p-1} \equiv 1 \pmod p}$$

Lemme 3

p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$, c'est-à-dire $\binom{p}{k} \equiv 0 \pmod p$.

Démonstration

$\binom{p}{k} = \frac{p!}{k!(p-k)!}$ donc $p! = k!(p-k)!\binom{p}{k}$. Ainsi $p|k!(p-k)!\binom{p}{k}$. Or comme $1 \leqslant k \leqslant p-1$ alors p ne divise pas $k!$ (sinon p divise l'un des facteurs de $k!$ mais il sont tous $< p$). De même p ne divise pas $(p-k)!$, donc par le lemme d'Euclide p divise $\binom{p}{k}$.

Démonstration . Preuve du théorème

Nous le montrons par récurrence pour les $a \geqslant 0$.

- Si $a = 0$ alors $0 \equiv 0 \pmod p$.
- Fixons $a \geqslant 0$ et supposons que $a^p \equiv a \pmod p$. Calculons $(a+1)^p$ à l'aide de la formule du binôme de Newton :

$$(a+1)^p = a^p + \binom{p}{p-1}a^{p-1} + \binom{p}{p-2}a^{p-2} + \cdots + \binom{p}{1} + 1$$

  Réduisons maintenant modulo p :

$$\begin{aligned}(a+1)^p &\equiv a^p + \binom{p}{p-1}a^{p-1} + \binom{p}{p-2}a^{p-2} + \cdots + \binom{p}{1} + 1 \pmod p \\ &\equiv a^p + 1 \pmod p \quad \text{grâce au lemme 3} \\ &\equiv a + 1 \pmod p \quad \text{à cause de l'hypothèse de récurrence}\end{aligned}$$

– Par le principe de récurrence nous avons démontré le petit théorème de Fermat pour tout $a \geqslant 0$. Il n'est pas dur d'en déduire le cas des $a \leqslant 0$.

Exemple 39

Calculons $14^{3141} \pmod{17}$. Le nombre 17 étant premier on sait par le petit théorème de Fermat que $14^{16} \equiv 1 \pmod{17}$. Écrivons la division euclidienne de 3141 par 16 :

$$3141 = 16 \times 196 + 5.$$

Alors

$$14^{3141} \equiv 14^{16\times196+5} \equiv 14^{16\times196} \times 14^5 \equiv \left(14^{16}\right)^{196} \times 14^5 \equiv 1^{196} \times 14^5 \equiv 14^5 \pmod{17}$$

Il ne reste plus qu'à calculer 14^5 modulo 17. Cela peut se faire rapidement : $14 \equiv -3 \pmod{17}$ donc $14^2 \equiv (-3)^2 \equiv 9 \pmod{17}$, $14^3 \equiv 14^2 \times 14 \equiv 9 \times (-3) \equiv -27 \equiv 7 \pmod{17}$, $14^5 \equiv 14^2 \times 14^3 \equiv 9 \times 7 \equiv 63 \equiv 12 \pmod{17}$. Conclusion : $14^{3141} \equiv 14^5 \equiv 12 \pmod{17}$.

Mini-exercices

1. Calculer les restes modulo 10 de $122+455$, 122×455, 122^{455}. Mêmes calculs modulo 11, puis modulo 12.
2. Prouver qu'un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.
3. Calculer $3^{10} \pmod{23}$.
4. Calculer $3^{100} \pmod{23}$.
5. Résoudre les équations $3x \equiv 4 \pmod 7$, $4x \equiv 14 \pmod{30}$.

Auteurs

Arnaud Bodin
Benjamin Boutin
Pascal Romon



5 Polynômes

Vidéo ■ partie 1. Définitions
Vidéo ■ partie 2. Arithmétique des polynômes
Vidéo ■ partie 3. Racine d'un polynôme, factorisation
Vidéo ■ partie 4. Fractions rationnelles
Exercices ♦ Polynômes

Motivation

Les polynômes sont des objets très simples mais aux propriétés extrêmement riches. Vous savez déjà résoudre les équations de degré 2 : $aX^2 + bX + c = 0$. Savez-vous que la résolution des équations de degré 3, $aX^3 + bX^2 + cX + d = 0$, a fait l'objet de luttes acharnées dans l'Italie du XVIe siècle ? Un concours était organisé avec un prix pour chacune de trente équations de degré 3 à résoudre. Un jeune italien, Tartaglia, trouve la formule générale des solutions et résout les trente équations en une seule nuit ! Cette méthode que Tartaglia voulait garder secrète sera quand même publiée quelques années plus tard comme la « méthode de Cardan ».
Dans ce chapitre, après quelques définitions des concepts de base, nous allons étudier l'arithmétique des polynômes. Il y a une grande analogie entre l'arithmétique des polynômes et celles des entiers. On continue avec un théorème fondamental de l'algèbre : « Tout polynôme de degré n admet n racines complexes. » On termine avec les fractions rationnelles : une fraction rationnelle est le quotient de deux polynômes.

Dans ce chapitre $\mathbb{K}$ désignera l'un des corps $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

1. Définitions

1.1. Définitions

Définition 19

Un ***polynôme*** à coefficients dans $\mathbb{K}$ est une expression de la forme

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0,$$

avec $n \in \mathbb{N}$ et $a_0, a_1, \ldots, a_n \in \mathbb{K}$.
L'ensemble des polynômes est noté $\mathbb{K}[X]$.

- Les a_i sont appelés les ***coefficients*** du polynôme.
- Si tous les coefficients a_i sont nuls, P est appelé le ***polynôme nul***, il est noté 0.
- On appelle le ***degré*** de P le plus grand entier i tel que $a_i \neq 0$; on le note $\deg P$. Pour

le degré du polynôme nul on pose par convention $\deg(0) = -\infty$.
- Un polynôme de la forme $P = a_0$ avec $a_0 \in \mathbb{K}$ est appelé un ***polynôme constant***. Si $a_0 \neq 0$, son degré est 0.

Exemple 40

- $X^3 - 5X + \frac{3}{4}$ est un polynôme de degré 3.
- $X^n + 1$ est un polynôme de degré n.
- 2 est un polynôme constant, de degré 0.

1.2. Opérations sur les polynômes

- **Égalité.** Soient $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ et $Q = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$ deux polynômes à coefficients dans $\mathbb{K}$.

$$P = Q \quad \text{ssi} \quad a_i = b_i \ \text{ pour tout } i$$

et on dit que P et Q sont égaux.
- **Addition.** Soient $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ et $Q = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$. On définit :

$$P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + \cdots + (a_1 + b_1)X + (a_0 + b_0)$$

- **Multiplication.** Soient $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ et $Q = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$. On définit

$$P \times Q = c_rX^r + c_{r-1}X^{r-1} + \cdots + c_1X + c_0 \text{ avec } r = n + m \text{ et } c_k = \sum_{i+j=k} a_ib_j \text{ pour } k \in \{0, \ldots, r\}.$$

- **Multiplication par un scalaire.** Si $\lambda \in \mathbb{K}$ alors $\lambda \cdot P$ est le polynôme dont le i-ème coefficient est λa_i.

Exemple 41

- Soient $P = aX^3 + bX^2 + cX + d$ et $Q = \alpha X^2 + \beta X + \gamma$. Alors $P + Q = aX^3 + (b + \alpha)X^2 + (c + \beta)X + (d + \gamma)$, $P \times Q = (a\alpha)X^5 + (a\beta + b\alpha)X^4 + (a\gamma + b\beta + c\alpha)X^3 + (b\gamma + c\beta + d\alpha)X^2 + (c\gamma + d\beta)X + d\gamma$. Enfin $P = Q$ si et seulement si $a = 0$, $b = \alpha$, $c = \beta$ et $d = \gamma$.
- La multiplication par un scalaire $\lambda \cdot P$ équivaut à multiplier le polynôme constant λ par le polynôme P.

L'addition et la multiplication se comportent sans problème :

Proposition 28

Pour $P, Q, R \in \mathbb{K}[X]$ alors
- $0 + P = P, \quad P + Q = Q + P, \quad (P + Q) + R = P + (Q + R)$;
- $1 \cdot P = P, \quad P \times Q = Q \times P, \quad (P \times Q) \times R = P \times (Q \times R)$;
- $P \times (Q + R) = P \times Q + P \times R$.

Pour le degré il faut faire attention :

Proposition 29

Soient P et Q deux polynômes à coefficients dans $\mathbb{K}$.

$$\boxed{\deg(P \times Q) = \deg P + \deg Q}$$

$$\boxed{\deg(P + Q) \leqslant \max(\deg P, \deg Q)}$$

On note $\mathbb{R}_n[X] = \{P \in \mathbb{R}[X] \mid \deg P \leqslant n\}$. Si $P, Q \in \mathbb{R}_n[X]$ alors $P + Q \in \mathbb{R}_n[X]$.

1.3. Vocabulaire

Complétons les définitions sur les polynômes.

Définition 20

- Les polynômes comportant un seul terme non nul (du type $a_k X^k$) sont appelés ***monômes***.
- Soit $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$, un polynôme avec $a_n \neq 0$. On appelle ***terme dominant*** le monôme $a_n X^n$. Le coefficient a_n est appelé le ***coefficient dominant*** de P.
- Si le coefficient dominant est 1, on dit que P est un ***polynôme unitaire***.

Exemple 42

$P(X) = (X-1)(X^n + X^{n-1} + \cdots + X + 1)$. On développe cette expression : $P(X) = \left(X^{n+1} + X^n + \cdots + X^2 + X\right) - \left(X^n + X^{n-1} + \cdots + X + 1\right) = X^{n+1} - 1$. $P(X)$ est donc un polynôme de degré $n+1$, il est unitaire et est somme de deux monômes : X^{n+1} et -1.

Remarque

Tout polynôme est donc une somme finie de monômes.

Mini-exercices

1. Soit $P(X) = 3X^3 - 2$, $Q(X) = X^2 + X - 1$, $R(X) = aX + b$. Calculer $P + Q$, $P \times Q$, $(P + Q) \times R$ et $P \times Q \times R$. Trouver a et b afin que le degré de $P - QR$ soit le plus petit possible.
2. Calculer $(X+1)^5 - (X-1)^5$.
3. Déterminer le degré de $(X^2 + X + 1)^n - aX^{2n} - bX^{2n-1}$ en fonction de a, b.
4. Montrer que si $\deg P \neq \deg Q$ alors $\deg(P + Q) = \max(\deg P, \deg Q)$. Donner un contre-exemple dans le cas où $\deg P = \deg Q$.
5. Montrer que si $P(X) = X^n + a_{n-1} X^{n-1} + \cdots$ alors le coefficient devant X^{n-1} de $P(X - \frac{a_{n-1}}{n})$ est nul.

2. Arithmétique des polynômes

Il existe de grandes similarités entre l'arithmétique dans $\mathbb{Z}$ et l'arithmétique dans $\mathbb{K}[X]$. Cela nous permet d'aller assez vite et d'omettre certaines preuves.

2.1. Division euclidienne

Définition 21

Soient $A,B \in \mathbb{K}[X]$, on dit que B ***divise*** A s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On note alors $B|A$.

On dit aussi que A est multiple de B ou que A est divisible par B.
Outre les propriétés évidentes comme $A|A$, $1|A$ et $A|0$ nous avons :

Proposition 30

Soient $A,B,C \in \mathbb{K}[X]$.

1. Si $A|B$ et $B|A$, alors il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.
2. Si $A|B$ et $B|C$ alors $A|C$.
3. Si $C|A$ et $C|B$ alors $C|(AU + BV)$, pour tout $U,V \in \mathbb{K}[X]$.

Théorème 7. Division euclidienne des polynômes

Soient $A,B \in \mathbb{K}[X]$, avec $B \neq 0$, alors il existe un unique polynôme Q et il existe un unique polynôme R tels que :

$$A = BQ + R \quad \text{et} \quad \deg R < \deg B.$$

Q est appelé le ***quotient*** et R le ***reste*** et cette écriture est la ***division euclidienne*** de A par B.
Notez que la condition $\deg R < \deg B$ signifie $R = 0$ ou bien $0 \leqslant \deg R < \deg B$.
Enfin $R = 0$ si et seulement si $B|A$.

Démonstration

Unicité. Si $A = BQ + R$ et $A = BQ' + R'$, alors $B(Q - Q') = R' - R$. Or $\deg(R' - R) < \deg B$. Donc $Q' - Q = 0$. Ainsi $Q = Q'$, d'où aussi $R = R'$.
Existence. On montre l'existence par récurrence sur le degré de A.

- Si $\deg A = 0$ et $\deg B > 0$, alors A est une constante, on pose $Q = 0$ et $R = A$. Si $\deg A = 0$ et $\deg B = 0$, on pose $Q = A/B$ et $R = 0$.
- On suppose l'existence vraie lorsque $\deg A \leqslant n-1$. Soit $A = a_n X^n + \cdots + a_0$ un polynôme de degré n ($a_n \neq 0$). Soit $B = b_m X^m + \cdots + b_0$ avec $b_m \neq 0$. Si $n < m$ on pose $Q = 0$ et $R = A$.
  Si $n \geqslant m$ on écrit $A = B \cdot \frac{a_n}{b_m} X^{n-m} + A_1$ avec $\deg A_1 \leqslant n-1$. On applique l'hypothèse de récurrence à A_1 : il existe $Q_1, R_1 \in \mathbb{K}[X]$ tels que $A_1 = BQ_1 + R_1$ et $\deg R_1 < \deg B$. Il vient :
  $$A = B\left(\frac{a_n}{b_m} X^{n-m} + Q_1\right) + R_1.$$
  Donc $Q = \frac{a_n}{b_m} X^{n-m} + Q_1$ et $R = R_1$ conviennent.

Exemple 43

On pose une division de polynômes comme on pose une division euclidienne de deux entiers. Par exemple si $A = 2X^4 - X^3 - 2X^2 + 3X - 1$ et $B = X^2 - X + 1$. Alors on trouve $Q = 2X^2 + X - 3$ et $R = -X + 2$. On n'oublie pas de vérifier qu'effectivement $A = BQ + R$.

$$
\begin{array}{rr|l}
 & 2X^4 - X^3 - 2X^2 + 3X - 1 & X^2 - X + 1 \\
- & 2X^4 - 2X^3 + 2X^2 & \\
\hline
 & X^3 - 4X^2 + 3X - 1 & 2X^2 + X - 3 \\
- & X^3 - X^2 + X & \\
\hline
 & -3X^2 + 2X - 1 & \\
- & -3X^2 + 3X - 3 & \\
\hline
 & -X + 2 &
\end{array}
$$

Exemple 44

Pour $X^4 - 3X^3 + X + 1$ divisé par $X^2 + 2$ on trouve un quotient égal à $X^2 - 3X - 2$ et un reste égale à $7X + 5$.

$$
\begin{array}{rr|l}
 & X^4 - 3X^3 + X + 1 & X^2 + 2 \\
- & X^4 + 2X^2 & \\
\hline
 & -3X^3 - 2X^2 + X + 1 & X^2 - 3X - 2 \\
- & -3X^3 - 6X & \\
\hline
 & -2X^2 + 7X + 1 & \\
- & -2X^2 - 4 & \\
\hline
 & 7X + 5 &
\end{array}
$$

2.2. pgcd

Proposition 31

Soient $A, B \in \mathbb{K}[X]$, avec $A \neq 0$ ou $B \neq 0$. Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois A et B.

Cet unique polynôme est appelé le ***pgcd*** (plus grand commun diviseur) de A et B que l'on note $\mathrm{pgcd}(A, B)$.

Remarque

- $\text{pgcd}(A,B)$ est un polynôme unitaire.
- Si $A|B$ et $A \neq 0$, $\text{pgcd}(A,B) = \frac{1}{\lambda}A$, où λ est le coefficient dominant de A.
- Pour tout $\lambda \in K^*$, $\text{pgcd}(\lambda A,B) = \text{pgcd}(A,B)$.
- Comme pour les entiers : si $A = BQ+R$ alors $\text{pgcd}(A,B) = \text{pgcd}(B,R)$. C'est ce qui justifie l'algorithme d'Euclide.

Algorithme d'Euclide. Soient A et B des polynômes, $B \neq 0$.
On calcule les divisions euclidiennes successives,

$$\begin{array}{ll}
A = BQ_1 + R_1 & \deg R_1 < \deg B \\
B = R_1Q_2 + R_2 & \deg R_2 < \deg R_1 \\
R_1 = R_2Q_3 + R_3 & \deg R_3 < \deg R_2 \\
\vdots & \\
R_{k-2} = R_{k-1}Q_k + R_k & \deg R_k < \deg R_{k-1} \\
R_{k-1} = R_kQ_{k+1} &
\end{array}$$

Le degré du reste diminue à chaque division. On arrête l'algorithme lorsque le reste est nul. Le pgcd est le dernier reste non nul R_k (rendu unitaire).

Exemple 45

Calculons le pgcd de $A = X^4 - 1$ et $B = X^3 - 1$. On applique l'algorithme d'Euclide :

$$\begin{array}{rcl}
X^4 - 1 & = & (X^3 - 1) \times X + X - 1 \\
X^3 - 1 & = & (X - 1) \times (X^2 + X + 1) + 0
\end{array}$$

Le pgcd est le dernier reste non nul, donc $\text{pgcd}(X^4 - 1, X^3 - 1) = X - 1$.

Exemple 46

Calculons le pgcd de $A = X^5 + X^4 + 2X^3 + X^2 + X + 2$ et $B = X^4 + 2X^3 + X^2 - 4$.

$$\begin{array}{rcl}
X^5 + X^4 + 2X^3 + X^2 + X + 2 & = & (X^4 + 2X^3 + X^2 - 4) \times (X - 1) + 3X^3 + 2X^2 + 5X - 2 \\
X^4 + 2X^3 + X^2 - 4 & = & (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X + 4) - \frac{14}{9}(X^2 + X + 2) \\
3X^3 + 2X^2 + 5X - 2 & = & (X^2 + X + 2) \times (3X - 1) + 0
\end{array}$$

Ainsi $\text{pgcd}(A,B) = X^2 + X + 2$.

Définition 22

Soient $A,B \in \mathbb{K}[X]$. On dit que A et B sont ***premiers entre eux*** si $\text{pgcd}(A,B) = 1$.

Pour A,B quelconques on peut se ramener à des polynômes premiers entre eux : si $\text{pgcd}(A,B) = D$ alors A et B s'écrivent : $A = DA'$, $B = DB'$ avec $\text{pgcd}(A',B') = 1$.

2.3. Théorème de Bézout

Théorème 8. Théorème de Bézout

Soient $A,B \in \mathbb{K}[X]$ des polynômes avec $A \neq 0$ ou $B \neq 0$. On note $D = \text{pgcd}(A,B)$. Il existe deux polynômes $U,V \in \mathbb{K}[X]$ tels que $AU + BV = D$.

Ce théorème découle de l'algorithme d'Euclide et plus spécialement de sa remontée comme on le voit sur l'exemple suivant.

Exemple 47

Nous avons calculé $\text{pgcd}(X^4-1, X^3-1) = X-1$. Nous remontons l'algorithme d'Euclide, ici il n'y avait qu'une ligne : $X^4-1 = (X^3-1)\times X + X - 1$, pour en déduire $X-1 = (X^4-1)\times 1 + (X^3-1)\times(-X)$. Donc $U = 1$ et $V = -X$ conviennent.

Exemple 48

Pour $A = X^5+X^4+2X^3+X^2+X+2$ et $B = X^4+2X^3+X^2-4$ nous avions trouvé $D = \text{pgcd}(A,B) = X^2+X+2$. En partant de l'avant dernière ligne de l'algorithme d'Euclide on a d'abord : $B = (3X^3+2X^2+5X-2)\times\frac{1}{9}(3X+4) - \frac{14}{9}D$ donc

$$-\frac{14}{9}D = B - (3X^3+2X^2+5X-2)\times\frac{1}{9}(3X+4).$$

La ligne au-dessus dans l'algorithme d'Euclide était : $A = B\times(X-1)+3X^3+2X^2+5X-2$. On substitue le reste pour obtenir :

$$-\frac{14}{9}D = B - \big(A - B\times(X-1)\big)\times\frac{1}{9}(3X+4).$$

On en déduit

$$-\frac{14}{9}D = -A\times\frac{1}{9}(3X+4) + B\big(1+(X-1)\times\frac{1}{9}(3X+4)\big)$$

Donc en posant $U = \frac{1}{14}(3X+4)$ et $V = -\frac{1}{14}\big(9+(X-1)(3X+4)\big) = -\frac{1}{14}(3X^2+X+5)$ on a $AU+BV = D$.

Le corollaire suivant s'appelle aussi le théorème de Bézout.

Corollaire 6

Soient A et B deux polynômes. A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que $AU + BV = 1$.

Corollaire 7

Soient $A,B,C \in \mathbb{K}[X]$ avec $A \neq 0$ ou $B \neq 0$. Si $C|A$ et $C|B$ alors $C|\text{pgcd}(A,B)$.

Corollaire 8. Lemme de Gauss

Soient $A,B,C \in \mathbb{K}[X]$. Si $A|BC$ et $\text{pgcd}(A,B) = 1$ alors $A|C$.

2.4. ppcm

Proposition 32

Soient $A,B \in \mathbb{K}[X]$ des polynômes non nuls, alors il existe un unique polynôme unitaire M de plus petit degré tel que $A|M$ et $B|M$.

Cet unique polynôme est appelé le ***ppcm*** (plus petit commun multiple) de A et B qu'on note $\text{ppcm}(A,B)$.

Exemple 49

$\text{ppcm}\left(X(X-2)^2(X^2+1)^4,(X+1)(X-2)^3(X^2+1)^3\right) = X(X+1)(X-2)^3(X^2+1)^4.$

De plus le ppcm est aussi le plus petit au sens de la divisibilité :

Proposition 33

Soient $A,B \in \mathbb{K}[X]$ des polynômes non nuls et $M = \text{ppcm}(A,B)$. Si $C \in \mathbb{K}[X]$ est un polynôme tel que $A|C$ et $B|C$, alors $M|C$.

Mini-exercices

1. Trouver les diviseurs de X^4+2X^2+1 dans $\mathbb{R}[X]$, puis dans $\mathbb{C}[X]$.
2. Montrer que $X-1|X^n-1$ (pour $n \geqslant 1$).
3. Calculer les divisions euclidiennes de A par B avec $A = X^4-1$, $B = X^3-1$. Puis $A = 4X^3+2X^2-X-5$ et $B = X^2+X$; $A = 2X^4-9X^3+18X^2-21X+2$ et $B = X^2-3X+1$; $A = X^5-2X^4+6X^3$ et $B = 2X^3+1$.
4. Déterminer le pgcd de $A = X^5+X^3+X^2+1$ et $B = 2X^3+3X^2+2X+3$. Trouver les coefficients de Bézout U,V. Mêmes questions avec $A = X^5-1$ et $B = X^4+X+1$.
5. Montrer que si $AU+BV = 1$ avec $\deg U < \deg B$ et $\deg V < \deg A$ alors les polynômes U,V sont uniques.

3. Racine d'un polynôme, factorisation

3.1. Racines d'un polynôme

Définition 23

Soit $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$. Pour un élément $x \in \mathbb{K}$, on note $P(x) = a_n x^n + \cdots + a_1 x + a_0$. On associe ainsi au polynôme P une ***fonction polynôme*** (que l'on note encore P)

$$P : \mathbb{K} \to \mathbb{K}, \quad x \mapsto P(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Définition 24

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On dit que α est une ***racine*** (ou un ***zéro***) de P si $P(\alpha) = 0$.

Proposition 34

$$P(\alpha) = 0 \quad \iff \quad X - \alpha \text{ divise } P$$

Démonstration

Lorsque l'on écrit la division euclidienne de P par $X - \alpha$ on obtient $P = Q \cdot (X - \alpha) + R$ où R est une constante car $\deg R < \deg(X - \alpha) = 1$. Donc $P(\alpha) = 0 \iff R(\alpha) = 0 \iff R = 0 \iff X - \alpha | P$.

Définition 25

Soit $k \in \mathbb{N}^*$. On dit que α est une ***racine de multiplicité k*** de P si $(X - \alpha)^k$ divise P alors que $(X - \alpha)^{k+1}$ ne divise pas P. Lorsque $k = 1$ on parle d'une ***racine simple***, lorsque $k = 2$ d'une ***racine double***, etc.

On dit aussi que α est une ***racine d'ordre k***.

Proposition 35

Il y a équivalence entre :

(i) α est une racine de multiplicité k de P.

(ii) Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)^k Q$, avec $Q(\alpha) \neq 0$.

(iii) $P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0$ et $P^{(k)}(\alpha) \neq 0$.

Remarque

Par analogie avec la dérivée d'une fonction, si $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ alors le polynôme $P'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}$ est le ***polynôme dérivé*** de P.

3.2. Théorème de d'Alembert-Gauss

Passons à un résultat essentiel de ce chapitre :

Théorème 9. Théorème de d'Alembert-Gauss

Tout polynôme à coefficients complexes de degré $n \geqslant 1$ a au moins une racine dans $\mathbb{C}$. Il admet exactement n racines si on compte chaque racine avec multiplicité.

Nous admettons ce théorème.

Exemple 50

Soit $P(X) = aX^2 + bX + c$ un polynôme de degré 2 à coefficients réels : $a, b, c \in \mathbb{R}$ et $a \neq 0$.

- Si $\Delta = b^2 - 4ac > 0$ alors P admet 2 racines réelles distinctes $\frac{-b+\sqrt{\Delta}}{2a}$ et $\frac{-b-\sqrt{\Delta}}{2a}$.
- Si $\Delta < 0$ alors P admet 2 racines complexes distinctes $\frac{-b+\mathrm{i}\sqrt{|\Delta|}}{2a}$ et $\frac{-b-\mathrm{i}\sqrt{|\Delta|}}{2a}$.
- Si $\Delta = 0$ alors P admet une racine réelle double $\frac{-b}{2a}$.

En tenant compte des multiplicités on a donc toujours exactement 2 racines.

Exemple 51

$P(X) = X^n - 1$ admet n racines distinctes.

Sachant que P est de degré n alors par le théorème de d'Alembert-Gauss on sait qu'il admet n racines comptées avec multiplicité. Il s'agit donc maintenant de montrer que ce sont des racines simples. Supposons –par l'absurde– que $\alpha \in \mathbb{C}$ soit une racine de multiplicité $\geqslant 2$. Alors $P(\alpha) = 0$ et $P'(\alpha) = 0$. Donc $\alpha^n - 1 = 0$ et $n\alpha^{n-1} = 0$. De la seconde égalité on déduit $\alpha = 0$, contradictoire avec la première égalité. Donc toutes les racines sont simples. Ainsi les n racines sont distinctes. (Remarque : sur cet exemple particulier on aurait aussi pu calculer les racines qui sont ici les racines n-ième de l'unité.)

Pour les autres corps que les nombres complexes nous avons le résultat plus faible suivant :

Théorème 10

Soit $P \in \mathbb{K}[X]$ de degré $n \geqslant 1$. Alors P admet au plus n racines dans $\mathbb{K}$.

Exemple 52

$P(X) = 3X^3 - 2X^2 + 6X - 4$. Considéré comme un polynôme à coefficients dans $\mathbb{Q}$ ou $\mathbb{R}$, P n'a qu'une seule racine (qui est simple) $\alpha = \frac{2}{3}$ et il se décompose en $P(X) = 3(X - \frac{2}{3})(X^2 + 2)$. Si on considère maintenant P comme un polynôme à coefficients dans $\mathbb{C}$ alors $P(X) = 3(X - \frac{2}{3})(X - \mathrm{i}\sqrt{2})(X + \mathrm{i}\sqrt{2})$ et admet 3 racines simples.

3.3. Polynômes irréductibles

Définition 26

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $\geqslant 1$, on dit que P est ***irréductible*** si pour tout $Q \in \mathbb{K}[X]$ divisant P, alors, soit $Q \in \mathbb{K}^*$, soit il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.

Remarque

- Un polynôme irréductible P est donc un polynôme non constant dont les seuls diviseurs de P sont les constantes ou P lui-même (à une constante multiplicative près).
- La notion de polynôme irréductible pour l'arithmétique de $\mathbb{K}[X]$ correspond à la notion de nombre premier pour l'arithmétique de $\mathbb{Z}$.
- Dans le cas contraire, on dit que P est ***réductible*** ; il existe alors des polynômes A,B de $\mathbb{K}[X]$ tels que $P = AB$, avec $\deg A \geqslant 1$ et $\deg B \geqslant 1$.

Exemple 53

- Tous les polynômes de degré 1 sont irréductibles. Par conséquent il y a une infinité de polynômes irréductibles.
- $X^2 - 1 = (X-1)(X+1) \in \mathbb{R}[X]$ est réductible.
- $X^2 + 1 = (X-\mathrm{i})(X+\mathrm{i})$ est réductible dans $\mathbb{C}[X]$ mais est irréductible dans $\mathbb{R}[X]$.
- $X^2 - 2 = (X-\sqrt{2})(X+\sqrt{2})$ est réductible dans $\mathbb{R}[X]$ mais est irréductible dans $\mathbb{Q}[X]$.

Nous avons l'équivalent du lemme d'Euclide de $\mathbb{Z}$ pour les polynômes :

Proposition 36. Lemme d'Euclide

Soit $P \in \mathbb{K}[X]$ un polynôme irréductible et soient $A,B \in \mathbb{K}[X]$. Si $P|AB$ alors $P|A$ ou $P|B$.

Démonstration

Si P ne divise pas A alors $\mathrm{pgcd}(P,A) = 1$ car P est irréductible. Donc, par le lemme de Gauss, P divise B.

3.4. Théorème de factorisation

Théorème 11

Tout polynôme non constant $A \in \mathbb{K}[X]$ s'écrit comme un produit de polynômes irréductibles unitaires :

$$A = \lambda P_1^{k_1} P_2^{k_2} \cdots P_r^{k_r}$$

où $\lambda \in \mathbb{K}^*$, $r \in \mathbb{N}^*$, $k_i \in \mathbb{N}^*$ et les P_i sont des polynômes irréductibles distincts.
De plus cette décomposition est unique à l'ordre près des facteurs.

Il s'agit bien sûr de l'analogue de la décomposition d'un nombre en facteurs premiers.

3.5. Factorisation dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Théorème 12

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
Donc pour $P \in \mathbb{C}[X]$ de degré $n \geqslant 1$ la factorisation s'écrit $P = \lambda(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\cdots(X-\alpha_r)^{k_r}$, où $\alpha_1,\dots,\alpha_r$ sont les racines distinctes de P et $k_1,\dots,k_r$ sont leurs multiplicités.

Démonstration

Ce théorème résulte du théorème de d'Alembert-Gauss.

Théorème 13

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 ainsi que les polynômes de degré 2 ayant un discriminant $\Delta < 0$.
Soit $P \in \mathbb{R}[X]$ de degré $n \geqslant 1$. Alors la factorisation s'écrit $P = \lambda(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\cdots(X-\alpha_r)^{k_r}Q_1^{\ell_1}\cdots Q_s^{\ell_s}$, où les α_i sont exactement les racines réelles distinctes de multiplicité k_i et les Q_i sont des polynômes irréductibles de degré 2 : $Q_i = X^2+\beta_i X+\gamma_i$ avec $\Delta = \beta_i^2 - 4\gamma_i < 0$.

Exemple 54

$P(X) = 2X^4(X-1)^3(X^2+1)^2(X^2+X+1)$ est déjà décomposé en facteurs irréductibles dans $\mathbb{R}[X]$ alors que sa décomposition dans $\mathbb{C}[X]$ est $P(X) = 2X^4(X-1)^3(X-\mathrm{i})^2(X+\mathrm{i})^2(X-j)(X-j^2)$ où $j = e^{\frac{2\mathrm{i}\pi}{3}} = \frac{-1+\mathrm{i}\sqrt{3}}{2}$.

Exemple 55

Soit $P(X) = X^4+1$.

- Sur $\mathbb{C}$. On peut d'abord décomposer $P(X) = (X^2+\mathrm{i})(X^2-\mathrm{i})$. Les racines de P sont donc les racines carrées complexes de i et −i. Ainsi P se factorise dans $\mathbb{C}[X]$:
$$P(X) = \Big(X-\tfrac{\sqrt{2}}{2}(1+\mathrm{i})\Big)\Big(X+\tfrac{\sqrt{2}}{2}(1+\mathrm{i})\Big)\Big(X-\tfrac{\sqrt{2}}{2}(1-\mathrm{i})\Big)\Big(X+\tfrac{\sqrt{2}}{2}(1-\mathrm{i})\Big).$$
- Sur $\mathbb{R}$. Pour un polynôme à coefficient réels, si α est une racine alors $\bar{\alpha}$ aussi. Dans la décomposition ci-dessus on regroupe les facteurs ayant des racines conjuguées, cela doit conduire à un polynôme réel :
$$P(X) = \Big[\Big(X-\tfrac{\sqrt{2}}{2}(1+\mathrm{i})\Big)\Big(X-\tfrac{\sqrt{2}}{2}(1-\mathrm{i})\Big)\Big]\Big[\Big(X+\tfrac{\sqrt{2}}{2}(1+\mathrm{i})\Big)\Big(X+\tfrac{\sqrt{2}}{2}(1-\mathrm{i})\Big)\Big] = [X^2+\sqrt{2}X+1][X^2-\sqrt{2}X+1],$$
qui est la factorisation dans $\mathbb{R}[X]$.

Mini-exercices

1. Trouver un polynôme $P(X) \in \mathbb{Z}[X]$ de degré minimal tel que : $\frac{1}{2}$ soit une racine simple, $\sqrt{2}$ soit une racine double et i soit une racine triple.
2. Montrer cette partie de la proposition 35 : « $P(\alpha) = 0$ et $P'(\alpha) = 0 \iff \alpha$ est une racine de multiplicité $\geqslant 2$ ».
3. Montrer que pour $P \in \mathbb{C}[X]$: « P admet une racine de multiplicité $\geqslant 2 \iff P$ et P' ne sont pas premiers entre eux ».

4. Factoriser $P(X) = (2X^2+X-2)^2(X^4-1)^3$ et $Q(X) = 3(X^2-1)^2(X^2-X+\frac{1}{4})$ dans $\mathbb{C}[X]$. En déduire leur pgcd et leur ppcm. Mêmes questions dans $\mathbb{R}[X]$.
5. Si $\mathrm{pgcd}(A,B) = 1$ montrer que $\mathrm{pgcd}(A+B, A\times B) = 1$.
6. Soit $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}\setminus\mathbb{R}$ tel que $P(\alpha) = 0$. Vérifier que $P(\bar{\alpha}) = 0$. Montrer que $(X-\alpha)(X-\bar{\alpha})$ est un polynôme irréductible de $\mathbb{R}[X]$ et qu'il divise P dans $\mathbb{R}[X]$.

4. Fractions rationnelles

Définition 27

Une ***fraction rationnelle*** à coefficients dans $\mathbb{K}$ est une expression de la forme

$$F = \frac{P}{Q}$$

où $P, Q \in \mathbb{K}[X]$ sont deux polynômes et $Q \neq 0$.

Toute fraction rationnelle se décompose comme une somme de fractions rationnelles élémentaires que l'on appelle des « éléments simples ». Mais les éléments simples sont différents sur $\mathbb{C}$ ou sur $\mathbb{R}$.

4.1. Décomposition en éléments simples sur $\mathbb{C}$

Théorème 14. Décomposition en éléments simples sur $\mathbb{C}$

Soit P/Q une fraction rationnelle avec $P, Q \in \mathbb{C}[X]$, $\mathrm{pgcd}(P,Q) = 1$ et $Q = (X-\alpha_1)^{k_1}\cdots(X-\alpha_r)^{k_r}$. Alors il existe une et une seule écriture :

$$\begin{aligned}\frac{P}{Q} = E & + \frac{a_{1,1}}{(X-\alpha_1)^{k_1}} + \frac{a_{1,2}}{(X-\alpha_1)^{k_1-1}} + \cdots + \frac{a_{1,k_1}}{(X-\alpha_1)} \\ & + \frac{a_{2,1}}{(X-\alpha_2)^{k_2}} + \cdots + \frac{a_{2,k_2}}{(X-\alpha_2)} \\ & + \cdots\end{aligned}$$

Le polynôme E s'appelle la ***partie polynomiale*** (ou ***partie entière***). Les termes $\frac{a}{(X-\alpha)^i}$ sont les ***éléments simples*** sur $\mathbb{C}$.

Exemple 56

- Vérifier que $\frac{1}{X^2+1} = \frac{a}{X+\mathrm{i}} + \frac{b}{X-\mathrm{i}}$ avec $a = \frac{1}{2}\mathrm{i}$, $b = -\frac{1}{2}\mathrm{i}$.
- Vérifier que $\frac{X^4-8X^2+9X-7}{(X-2)^2(X+3)} = X+1+\frac{-1}{(X-2)^2}+\frac{2}{X-2}+\frac{-1}{X+3}$.

Comment se calcule cette décomposition ? En général on commence par déterminer la partie polynomiale. Tout d'abord si $\deg Q > \deg P$ alors $E(X) = 0$. Si $\deg P \leqslant \deg Q$ alors effectuons la division euclidienne de P par Q : $P = QE + R$ donc $\frac{P}{Q} = E + \frac{R}{Q}$ où $\deg R < \deg Q$. La partie polynomiale est donc le quotient de cette division. Et on s'est ramené au cas d'une fraction $\frac{R}{Q}$ avec $\deg R < \deg Q$. Voyons en détails comment continuer sur un exemple.

Exemple 57

Décomposons la fraction $\frac{P}{Q} = \frac{X^5-2X^3+4X^2-8X+11}{X^3-3X+2}$.

- **Première étape : partie polynomiale.** On calcule la division euclidienne de P par Q : $P(X) = (X^2+1)Q(X) + 2X^2 - 5X + 9$. Donc la partie polynomiale est $E(X) = X^2+1$ et la fraction s'écrit $\frac{P(X)}{Q(X)} = X^2+1+\frac{2X^2-5X+9}{Q(X)}$. Notons que pour la fraction $\frac{2X^2-5X+9}{Q(X)}$ le degré du numérateur est strictement plus petit que le degré du dénominateur.
- **Deuxième étape : factorisation du dénominateur.** Q a pour racine évidente $+1$ (racine double) et -2 (racine simple) et se factorise donc ainsi $Q(X) = (X-1)^2(X+2)$.
- **Troisième étape : décomposition théorique en éléments simples.** Le théorème de décomposition en éléments simples nous dit qu'il existe une unique décomposition : $\frac{P(X)}{Q(X)} = E(X) + \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$. Nous savons déjà que $E(X) = X^2+1$, il reste à trouver les nombres a, b, c.
- **Quatrième étape : détermination des coefficients.** Voici une première façon de déterminer a, b, c. On récrit la fraction $\frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$ au même dénominateur et on l'identifie avec $\frac{2X^2-5X+9}{Q(X)}$:

$$\frac{a}{(X-1)^2}+\frac{b}{X-1}+\frac{c}{X+2} = \frac{(b+c)X^2+(a+b-2c)X+2a-2b+c}{(X-1)^2(X+2)} \text{ qui doit être égale à } \frac{2X^2-5X+9}{(X-1)^2(X+2)}.$$

  On en déduit $b+c=2$, $a+b-2c=-5$ et $2a-2b+c=9$. Cela conduit à l'unique solution $a=2$, $b=-1$, $c=3$. Donc

$$\frac{P}{Q} = \frac{X^5-2X^3+4X^2-8X+11}{X^3-3X+2} = X^2+1+\frac{2}{(X-1)^2}+\frac{-1}{X-1}+\frac{3}{X+2}.$$

  Cette méthode est souvent la plus longue.
- **Quatrième étape (bis) : détermination des coefficients.** Voici une autre méthode plus efficace.
  Notons $\frac{P'(X)}{Q(X)} = \frac{2X^2-5X+9}{(X-1)^2(X+2)}$ dont la décomposition théorique est : $\frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$
  Pour déterminer a on multiplie la fraction $\frac{P'}{Q}$ par $(X-1)^2$ et on évalue en $x=1$.
  Tout d'abord en partant de la décomposition théorique on a :

$$F_1(X) = (X-1)^2\frac{P'(X)}{Q(X)} = a + b(X-1) + c\frac{(X-1)^2}{X+2} \qquad \text{donc} \qquad F_1(1) = a$$

  D'autre part

$$F_1(X) = (X-1)^2\frac{P'(X)}{Q(X)} = (X-1)^2\frac{2X^2-5X+9}{(X-1)^2(X+2)} = \frac{2X^2-5X+9}{X+2} \text{ donc } F_1(1) = 2$$

  On en déduit $a=2$.
  On fait le même processus pour déterminer c : on multiplie par $(X+2)$ et on évalue en -2. On calcule $F_2(X) = (X+2)\frac{P'(X)}{Q(X)} = \frac{2X^2-5X+9}{(X-1)^2} = a\frac{X+2}{(X-1)^2} + b\frac{X+2}{X-1} + c$ de deux façons et lorsque l'on évalue $x=-2$ on obtient d'une part $F_2(-2) = c$ et d'autre part $F_2(-2) = 3$. Ainsi $c = 3$.
  Comme les coefficients sont uniques tous les moyens sont bons pour les déterminer. Par exemple lorsque l'on évalue la décomposition théorique $\frac{P'(X)}{Q(X)} = \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$ en $x=0$, on obtient :

$$\frac{P'(0)}{Q(0)} = a - b + \frac{c}{2}$$

Donc $\frac{9}{2} = a - b + \frac{c}{2}$. Donc $b = a + \frac{c}{2} - \frac{9}{2} = -1$.

4.2. Décomposition en éléments simples sur $\mathbb{R}$

Théorème 15. Décomposition en éléments simples sur $\mathbb{R}$

Soit P/Q une fraction rationnelle avec $P, Q \in \mathbb{R}[X]$, $\text{pgcd}(P,Q) = 1$. Alors P/Q s'écrit de manière unique comme somme :

- d'une partie polynomiale $E(X)$,
- d'éléments simples du type $\frac{a}{(X-\alpha)^i}$,
- d'éléments simples du type $\frac{aX+b}{(X^2+\alpha X+\beta)^i}$.

Où les $X - \alpha$ et $X^2 + \alpha X + \beta$ sont les facteurs irréductibles de $Q(X)$ et les exposants i sont inférieurs ou égaux à la puissance correspondante dans cette factorisation.

Exemple 58

Décomposition en éléments simples de $\frac{P(X)}{Q(X)} = \frac{3X^4+5X^3+8X^2+5X+3}{(X^2+X+1)^2(X-1)}$. Comme $\deg P < \deg Q$ alors $E(X) = 0$. Le dénominateur est déjà factorisé sur $\mathbb{R}$ car $X^2 + X + 1$ est irréductible. La décomposition théorique est donc :

$$\frac{P(X)}{Q(X)} = \frac{aX+b}{(X^2+X+1)^2} + \frac{cX+d}{X^2+X+1} + \frac{e}{X-1}.$$

Il faut ensuite mener au mieux les calculs pour déterminer les coefficients afin d'obtenir :

$$\frac{P(X)}{Q(X)} = \frac{2X+1}{(X^2+X+1)^2} + \frac{-1}{X^2+X+1} + \frac{3}{X-1}.$$

Mini-exercices

1. Soit $Q(X) = (X-2)^2(X^2-1)^3(X^2+1)^4$. Pour $P \in \mathbb{R}[X]$ quelle est la forme théorique de la décomposition en éléments simples sur $\mathbb{C}$ de $\frac{P}{Q}$? Et sur $\mathbb{R}$?
2. Décomposer les fractions suivantes en éléments simples sur $\mathbb{R}$ et $\mathbb{C}$: $\frac{1}{X^2-1}$; $\frac{X^2+1}{(X-1)^2}$; $\frac{X}{X^3-1}$.
3. Décomposer les fractions suivantes en éléments simples sur $\mathbb{R}$: $\frac{X^2+X+1}{(X-1)(X+2)^2}$; $\frac{2X^2-X}{(X^2+2)^2}$; $\frac{X^6}{(X^2+1)^2}$.
4. Soit $F(X) = \frac{2X^2+7X-20}{X+2}$. Déterminer l'équation de l'asymptote oblique en $\pm\infty$. Étudier la position du graphe de F par rapport à cette droite.

Auteurs

Rédaction : Arnaud Bodin
Basé sur des cours de Guoting Chen et Marc Bourdon
Relecture : Stéphanie Bodin



6 Les nombres réels

Exercices ♦ Propriétés de $\mathbb{R}$

Motivation

Voici une introduction, non seulement à ce chapitre sur les nombres réels, mais aussi aux premiers chapitres de ce cours d'analyse.
Aux temps des babyloniens (en Mésopotamie de 3000 à 600 avant J.C.) le système de numération était en base 60, c'est-à-dire que tous les nombres étaient exprimés sous la forme $a + \frac{b}{60} + \frac{c}{60^2} + \cdots$. On peut imaginer que pour les applications pratiques c'était largement suffisant (par exemple estimer la surface d'un champ, le diviser en deux parties égales, calculer le rendement par unité de surface,...). En langage moderne cela correspond à compter uniquement avec des nombres rationnels $\mathbb{Q}$.

Les pythagoriciens (vers 500 avant J.C. en Grèce) montrent que $\sqrt{2}$ n'entre pas ce cadre là. C'est-à-dire que $\sqrt{2}$ ne peut s'écrire sous la forme $\frac{p}{q}$ avec p et q deux entiers. C'est un double saut conceptuel : d'une part concevoir que $\sqrt{2}$ est de nature différente mais surtout d'en donner une démonstration.

Le fil rouge de ce cours va être deux exemples très simples : les nombres $\sqrt{10}$ et $1,10^{1/12}$. Le premier représente par exemple la diagonale d'un rectangle de base 3 et de hauteur 1 ; le second correspond par exemple au taux d'intérêt mensuel d'un taux annuel de 10%. Dans ce premier chapitre vous allez apprendre à montrer que $\sqrt{10}$ n'est pas un nombre rationnel mais aussi à encadrer $\sqrt{10}$ et $1,10^{1/12}$ entre deux entiers consécutifs.

Pour pouvoir calculer des décimales après la virgule, voire des centaines de décimales, nous aurons besoin d'outils beaucoup plus sophistiqués :
- une construction solide des nombres réels,
- l'étude des suites et de leur limites,
- l'étude des fonctions continues et des fonctions dérivables.

Ces trois points sont liés et permettent de répondre à notre problème, car par exemple nous verrons en étudiant la fonction $f(x) = x^2 - 10$ que la suite des rationnels (u_n) définie par $u_0 = 3$ et $u_{n+1} = \frac{1}{2}\left(u_n + \frac{10}{u_n}\right)$ tend très vite vers $\sqrt{10}$. Cela nous permettra de calculer des centaines de décimales de $\sqrt{10}$ et de certifier quelles sont exactes :

$$\sqrt{10} = 3,1622776601683793319988935444327185337195551393252168\ldots$$

1. L'ensemble des nombres rationnels $\mathbb{Q}$

1.1. Écriture décimale

Par définition, l'ensemble des ***nombres rationnels*** est

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N}^* \right\}.$$

On a noté $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.
Par exemple : $\frac{2}{5}$; $\frac{-7}{10}$; $\frac{3}{6} = \frac{1}{2}$.
Les nombres décimaux, c'est-à-dire les nombres de la forme $\frac{a}{10^n}$, avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$, fournissent d'autres exemples :

$$1,234 = 1234 \times 10^{-3} = \frac{1234}{1000} \qquad 0,00345 = 345 \times 10^{-5} = \frac{345}{100\,000}.$$

Proposition 37

Un nombre est rationnel si et seulement s'il admet une écriture décimale périodique ou finie.

Par exemple :

$$\frac{3}{5} = 0,6 \qquad \frac{1}{3} = 0,3333\ldots \qquad 1,179\underleftrightarrow{325}\,\underleftrightarrow{325}\,\underleftrightarrow{325}\ldots$$

Nous n'allons pas donner la démonstration mais le sens direct ($\Longrightarrow$) repose sur la division euclidienne. Pour la réciproque ($\Longleftarrow$) voyons comment cela marche sur un exemple : Montrons que $x = 12,34\underleftrightarrow{2021}\,\underleftrightarrow{2021}\ldots$ est un rationnel.
L'idée est d'abord de faire apparaître la partie périodique juste après la virgule. Ici la période commence deux chiffres après la virgule donc on multiplie par 100 :

$$100x = 1234,\underleftrightarrow{2021}\,\underleftrightarrow{2021}\ldots \tag{6.1}$$

Maintenant on va décaler tout vers la gauche de la longueur d'une période, donc ici on multiplie par encore par 10 000 pour décaler de 4 chiffres :

$$10\,000 \times 100x = 1234\,2021,\underleftrightarrow{2021}\ldots \tag{6.2}$$

Les parties après la virgule des deux lignes (6.1) et (6.2) sont les mêmes, donc si on les soustrait en faisant (6.2)-(6.1) alors les parties décimales s'annulent :

$$10\,000 \times 100x - 100x = 12\,342\,021 - 1234$$

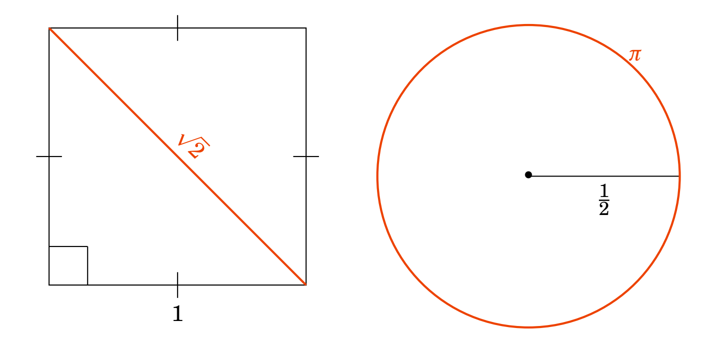
donc $999\,900x = 12\,340\,787$ donc

$$x = \frac{12\,340\,787}{999\,900}.$$

Et donc bien sûr $x \in \mathbb{Q}$.

1.2. $\sqrt{2}$ n'est pas un nombre rationnel

Il existe des nombres qui ne sont pas rationnels, les ***irrationnels***. Les nombres irrationnels apparaissent naturellement dans les figures géométriques : par exemple la diagonale d'un carré de côté 1 est le nombre irrationnel $\sqrt{2}$; la circonférence d'un cercle de rayon $\frac{1}{2}$ est π qui est également un nombre irrationnel. Enfin $e = \exp(1)$ est aussi irrationnel.



Nous allons prouver que $\sqrt{2}$ n'est pas un nombre rationnel.

Proposition 38

$$\boxed{\sqrt{2} \notin \mathbb{Q}}$$

Démonstration

Par l'absurde supposons que $\sqrt{2}$ soit un nombre rationnel. Alors il existe des entiers $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $\sqrt{2} = \frac{p}{q}$, de plus –ce sera important pour la suite– on suppose que p et q sont premiers entre eux (c'est-à-dire que la fraction $\frac{p}{q}$ est sous une écriture irréductible).
En élevant au carré, l'égalité $\sqrt{2} = \frac{p}{q}$ devient $2q^2 = p^2$. Cette dernière égalité est une égalité d'entiers. L'entier de gauche est pair, donc on en déduit que p^2 est pair ; en terme de divisibilité 2 divise p^2.
Mais si 2 divise p^2 alors 2 divise p (cela se prouve par facilement l'absurde). Donc il existe un entier $p' \in \mathbb{Z}$ tel que $p = 2p'$.
Repartons de l'égalité $2q^2 = p^2$ et remplaçons p par $2p'$. Cela donne $2q^2 = 4p'^2$. Donc $q^2 = 2p'^2$. Maintenant cela entraîne que 2 divise q^2 et comme avant alors 2 divise q.
Nous avons prouvé que 2 divise à la fois p et q. Cela rentre en contradiction avec le fait que p et q sont premiers entre eux. Notre hypothèse de départ est donc fausse : $\sqrt{2}$ n'est pas un nombre rationnel.

Comme ce résultat est important en voici une deuxième démonstration, assez différente mais toujours par l'absurde.

Démonstration . Autre démonstration

Par l'absurde, supposons $\sqrt{2} = \frac{p}{q}$, donc $q\sqrt{2} = p \in \mathbb{N}$. Considérons l'ensemble

$$\mathcal{N} = \left\{ n \in \mathbb{N}^* \mid n\sqrt{2} \in \mathbb{N} \right\}.$$

Cet ensemble n'est pas vide car on vient de voir que $q\sqrt{2} = p \in \mathbb{N}$ donc $q \in \mathcal{N}$. Ainsi $\mathcal{N}$ est une partie non vide de $\mathbb{N}$, elle admet donc un plus petit élément $n_0 = \min \mathcal{N}$.
Posons

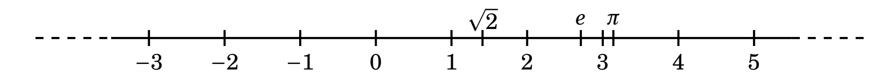
$$n_1 = n_0\sqrt{2} - n_0 = n_0(\sqrt{2} - 1),$$

il découle de cette dernière égalité et de $1 < \sqrt{2} < 2$ que $0 < n_1 < n_0$.
De plus $n_1\sqrt{2} = (n_0\sqrt{2} - n_0)\sqrt{2} = 2n_0 - n_0\sqrt{2} \in \mathbb{N}$. Donc $n_1 \in \mathcal{N}$ et $n_1 < n_0$: on vient de trouver un élément n_1 de $\mathcal{N}$ strictement plus petit que n_0 qui était le minimum. C'est une contradiction.
Notre hypothèse de départ est fausse, donc $\sqrt{2} \notin \mathbb{Q}$.

Exercice 1

Montrer que $\sqrt{10} \notin \mathbb{Q}$.

On représente souvent les nombres réels sur une « droite numérique » :



Il est bon de connaître les premières décimales de certains réels $\sqrt{2} \simeq 1,4142\ldots$ $\pi \simeq 3,14159265\ldots$ $e \simeq 2,718\ldots$

Il est souvent pratique de rajouter les deux extrémités à la droite numérique.

Définition 28

$$\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$$

Mini-exercices

1. Montrer que la somme de deux rationnels est un rationnel. Montrer que le produit de deux rationnels est un rationnel. Montrer que l'inverse d'un rationnel non nul est un rationnel. Qu'en est-il pour les irrationnels ?
2. Écrire les nombres suivants sous forme d'une fraction : $0,1212$; $0,12\overleftrightarrow{12}\ldots$; $78,33456\overleftrightarrow{456}\ldots$
3. Sachant $\sqrt{2} \notin \mathbb{Q}$, montrer $2-3\sqrt{2} \notin \mathbb{Q}$, $1-\frac{1}{\sqrt{2}} \notin \mathbb{Q}$.
4. Notons D l'ensemble des nombres de la forme $\frac{a}{2^n}$ avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$. Montrer que $3 \notin D$. Trouver $x \in D$ tel que $1234 < x < 1234,001$.
5. Montrer que $\frac{\sqrt{2}}{\sqrt{3}} \notin \mathbb{Q}$.
6. Montrer que $\log 2 \notin \mathbb{Q}$ ($\log 2$ est le logarithme décimal de 2 : c'est le nombre réel tel que $10^{\log 2} = 2$).

2. Propriétés de $\mathbb{R}$

2.1. Addition et multiplication

Ce sont les propriétés que vous avez toujours pratiquées. Pour $a, b, c \in \mathbb{R}$ on a :

$$\begin{array}{ll}
a+b=b+a & a\times b=b\times a \\
0+a=a & 1\times a=a \text{ si } a\neq 0 \\
a+b=0 \iff a=-b & ab=1 \iff a=\frac{1}{b} \\
(a+b)+c=a+(b+c) & (a\times b)\times c=a\times(b\times c)
\end{array}$$

$$a\times(b+c)=a\times b+a\times c$$
$$a\times b=0 \iff (a=0 \text{ ou } b=0)$$

On résume toutes ces propriétés en disant que :

Propriété : $\mathbb{R}1$

$(\mathbb{R},+,\times)$ est un ***corps commutatif***.

2.2. Ordre sur $\mathbb{R}$

Nous allons voir que les réels sont ordonnés. La notion d'ordre est générale et nous allons définir cette notion sur un ensemble quelconque. Cependant gardez à l'esprit que pour nous $E=\mathbb{R}$ et $\mathscr{R}=\leqslant$.

Définition 29

Soit E un ensemble.

1. Une ***relation*** $\mathscr{R}$ sur E est un sous-ensemble de l'ensemble produit $E\times E$. Pour $(x,y)\in E\times E$, on dit que x est en relation avec y et on note $x\mathscr{R}y$ pour dire que $(x,y)\in\mathscr{R}$.
2. Une relation $\mathscr{R}$ est une ***relation d'ordre*** si
   - $\mathscr{R}$ est ***réflexive*** : pour tout $x\in E$, $x\mathscr{R}x$,
   - $\mathscr{R}$ est ***antisymétrique*** : pour tout $x,y\in E$, $(x\mathscr{R}y \text{ et } y\mathscr{R}x)\implies x=y$,
   - $\mathscr{R}$ est ***transitive*** : pour tout $x,y,z\in E$, $(x\mathscr{R}y \text{ et } y\mathscr{R}z)\implies x\mathscr{R}z$.

Définition 30

Une relation d'ordre $\mathscr{R}$ sur un ensemble E est ***totale*** si pour tout $x,y\in E$ on a $x\mathscr{R}y$ ou $y\mathscr{R}x$. On dit aussi que $(E,\mathscr{R})$ est un ***ensemble totalement ordonné***.

Propriété : $\mathbb{R}2$

La relation $\leqslant$ sur $\mathbb{R}$ est une relation d'ordre, et de plus, elle est totale.

Nous avons donc :

- pour tout $x\in\mathbb{R}$, $x\leqslant x$,
- pour tout $x,y\in\mathbb{R}$, si $x\leqslant y$ et $y\leqslant x$ alors $x=y$,
- pour tout $x,y,z\in\mathbb{R}$ si $x\leqslant y$ et $y\leqslant z$ alors $x\leqslant z$.

Remarque

Pour $(x,y)\in\mathbb{R}^2$ on a par définition :

$$x\leqslant y \iff y-x\in\mathbb{R}_+$$
$$x<y \iff (x\leqslant y \text{ et } x\neq y).$$

Les opérations de $\mathbb{R}$ sont compatibles avec la relation d'ordre $\leqslant$ au sens suivant, pour des réels a,b,c,d :

$$(a\leqslant b \text{ et } c\leqslant d)\implies a+c\leqslant b+d$$
$$(a\leqslant b \text{ et } c\geqslant 0)\implies a\times c\leqslant b\times c$$
$$(a\leqslant b \text{ et } c\leqslant 0)\implies a\times c\geqslant b\times c.$$

On définit le maximum de deux réels a et b par :

$$\max(a,b)=\begin{cases} a & \text{si } a\geqslant b\\ b & \text{si } b>a.\end{cases}$$

Exercice 2

Comment définir $\max(a,b,c)$, $\max(a_1,a_2,\ldots,a_n)$? Et $\min(a,b)$?

2.3. Propriété d'Archimède

Propriété : ℝ3, Propriété d'Archimède

$\mathbb{R}$ est ***archimédien***, c'est-à-dire :

$$\forall x \in \mathbb{R} \ \ \exists n \in \mathbb{N} \ \ n > x$$

« Pour tout réel x, il existe un entier naturel n strictement plus grand que x. »

Cette propriété peut sembler évidente, elle est pourtant essentielle puisque elle permet de définir la ***partie entière*** d'un nombre réel :

Proposition 39

Soit $x \in \mathbb{R}$, il ***existe*** un ***unique*** entier relatif, la ***partie entière*** notée $E(x)$, tel que :

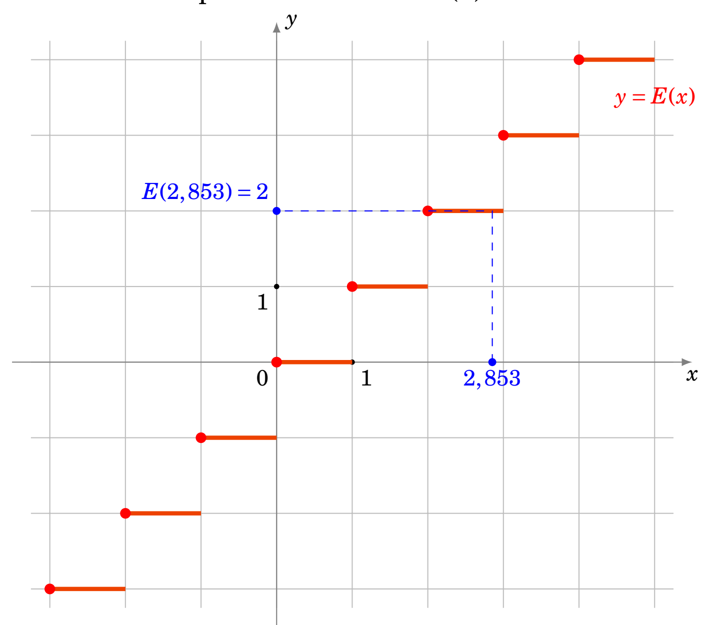
$$\boxed{E(x) \leqslant x < E(x)+1}$$

Exemple 59

- $E(2,853) = 2$, $E(\pi) = 3$, $E(-3,5) = -4$.
- $E(x) = 3 \iff 3 \leqslant x < 4$.

Remarque

- On note aussi $E(x) = [x]$.
- Voici le graphe de la fonction partie entière $x \mapsto E(x)$:



Pour la démonstration de la proposition 39 il y a deux choses à établir : d'abord qu'un tel entier $E(x)$ existe et ensuite qu'il est unique.

Démonstration

Existence. Supposons $x \geqslant 0$, par la propriété d'Archimède (Propriété ℝ3) il existe $n \in \mathbb{N}$ tel que $n > x$. L'ensemble $K = \{k \in \mathbb{N} \mid k \leqslant x\}$ est donc fini (car pour tout k dans K, on a $k < n$). Il admet donc un plus grand élément $k_{max} = \max K$. On alors $k_{max} \leqslant x$ car $k_{max} \in K$, et $k_{max} + 1 > x$ car $k_{max} + 1 \notin K$. Donc $k_{max} \leqslant x < k_{max} + 1$ et on prend donc $E(x) = k_{max}$.

Unicité. Si k et ℓ sont deux entiers relatifs vérifiant $k \leqslant x < k+1$ et $\ell \leqslant x < \ell + 1$, on a donc $k \leqslant x < \ell + 1$, donc par transitivité $k < \ell + 1$. En échangeant les rôles de ℓ et k, on a aussi $\ell < k + 1$. On en conclut que $\ell - 1 < k < \ell + 1$, mais il n'y a qu'un seul entier compris strictement entre $\ell - 1$ et $\ell + 1$, c'est ℓ. Ainsi $k = \ell$.

Exemple 60

Encadrons $\sqrt{10}$ et $1,1^{1/12}$ par deux entiers consécutifs.

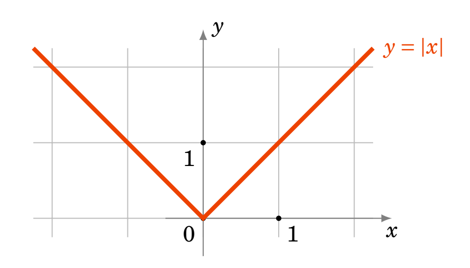
- Nous savons $3^2 = 9 < 10$ donc $3 = \sqrt{3^2} < \sqrt{10}$ (la fonction racine carrée est croissante). De même $4^2 = 16 > 10$ donc $4 = \sqrt{4^2} > \sqrt{10}$. Conclusion : $3 < \sqrt{10} < 4$ ce qui implique $E\left(\sqrt{10}\right) = 3$.
- On procède sur le même principe. $1^{12} < 1,10 < 2^{12}$ donc en passant à la racine 12-ième (c'est-à-dire à la puissance $\frac{1}{12}$) on obtient : $1 < 1,1^{1/12} < 2$ et donc $E\left(1,1^{1/12}\right) = 1$.

2.4. Valeur absolue

Pour un nombre réel x, on définit la ***valeur absolue*** de x par :

$$|x| = \begin{cases} x & \text{si } x \geqslant 0 \\ -x & \text{si } x < 0 \end{cases}$$

Voici le graphe de la fonction $x \mapsto |x|$:



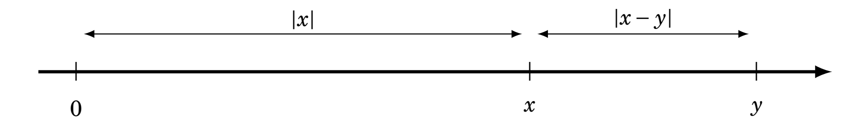
Proposition 40

1. $|x| \geqslant 0$; $|-x| = |x|$; $|x| > 0 \iff x \neq 0$
2. $\sqrt{x^2} = |x|$
3. $|xy| = |x||y|$
4. ***Inégalité triangulaire*** $|x + y| \leqslant |x| + |y|$
5. ***Seconde inégalité triangulaire*** $\big||x| - |y|\big| \leqslant |x - y|$

Démonstration . Démonstration des inégalités triangulaires

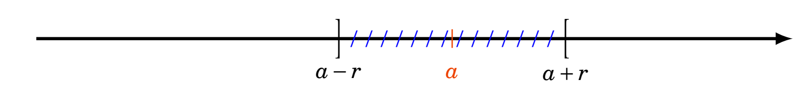
- $-|x| \leqslant x \leqslant |x|$ et $-|y| \leqslant y \leqslant |y|$. En additionnant $-(|x|+|y|) \leqslant x+y \leqslant |x|+|y|$, donc $|x+y| \leqslant |x|+|y|$.
- Puisque $x=(x-y)+y$, on a d'après la première inégalité : $|x| = \big|(x-y)+y\big| = \leqslant |x-y|+|y|$. Donc $|x|-|y| \leqslant |x-y|$, et en intervertissant les rôles de x et y, on a aussi $|y|-|x| \leqslant |y-x|$. Comme $|y-x| = |x-y|$ on a donc $\big||x|-|y|\big| \leqslant |x-y|$.

Sur la droite numérique, $|x-y|$ représente la distance entre les réels x et y ; en particulier $|x|$ représente la distance entre les réels x et 0.



De plus on a :

- $|x-a|<r \iff a-r<x<a+r$.
- Ou encore comme on le verra bientôt $|x-a|<r \iff x \in]a-r, a+r[$.



Exercice 3

Soit $a \in \mathbb{R}\setminus\{0\}$ et $x \in \mathbb{R}$ tel que $|x-a|<|a|$. Montrer que :

1. $x \neq 0$.
2. x est du signe de a.

Mini-exercices

1. On munit l'ensemble $\mathscr{P}(\mathbb{R})$ des parties de $\mathbb{R}$ de la relation $\mathscr{R}$ définie par $A\mathscr{R}B$ si $A \subset B$. Montrer qu'il s'agit d'une relation d'ordre. Est-elle totale ?
2. Soient x, y deux réels. Montrer que $|x| \geqslant \big||x+y|-|y|\big|$.
3. Soient $x_1, \ldots, x_n$ des réels. Montrer que $|x_1+\cdots+x_n| \leqslant |x_1|+\cdots+|x_n|$. Dans quel cas a-t-on égalité ?
4. Soient $x, y > 0$ des réels. Comparer $E(x+y)$ avec $E(x)+E(y)$. Comparer $E(x \times y)$ et $E(x) \times E(y)$.
5. Soit $x>0$ un réel. Encadrer $\frac{E(x)}{x}$. Quelle est la limite de $\frac{E(x)}{x}$ lorsque $x \to +\infty$?
6. On note $\{x\} = x - E(x)$ la *partie fractionnaire* de x, de sorte que $x = E(x)+\{x\}$. Représenter les graphes des fonctions $x \mapsto E(x)$, $x \mapsto \{x\}$, $x \mapsto E(x)-\{x\}$.

3. Densité de $\mathbb{Q}$ dans $\mathbb{R}$

3.1. Intervalle

Définition 31

Un ***intervalle de*** $\mathbb{R}$ est un sous-ensemble I de $\mathbb{R}$ vérifiant la propriété :

$$\forall a,b \in I \ \forall x \in \mathbb{R} \ (a \leqslant x \leqslant b \implies x \in I)$$

Remarque

- Par définition $I = \varnothing$ est un intervalle.
- $I = \mathbb{R}$ est aussi un intervalle.

Définition 32

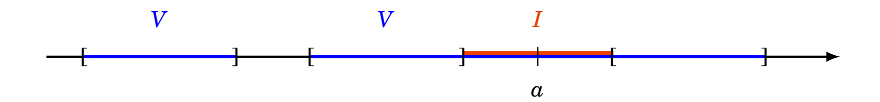
Un ***intervalle ouvert*** est un sous-ensemble de $\mathbb{R}$ de la forme $]a,b[= \{x \in \mathbb{R} \mid a < x < b\}$, où a et b sont des éléments de $\overline{\mathbb{R}}$.

Même si cela semble évident il faut justifier qu'un intervalle ouvert est un intervalle (!). En effet soient a', b' des éléments de $]a,b[$ et $x \in \mathbb{R}$ tel que $a' \leqslant x \leqslant b'$. Alors on a $a < a' \leqslant x \leqslant b' < b$, donc $x \in]a,b[$.

La notion de voisinage sera utile pour les limites.

Définition 33

Soit a un réel, $V \subset \mathbb{R}$ un sous-ensemble. On dit que V est un ***voisinage*** de a s'il existe un intervalle ouvert I tel que $a \in I$ et $I \subset V$.



3.2. Densité

Théorème 16

1. $\mathbb{Q}$ est ***dense*** dans $\mathbb{R}$: tout intervalle ouvert (non vide) de $\mathbb{R}$ contient une infinité de rationnels.
2. $\mathbb{R} \setminus \mathbb{Q}$ est dense dans $\mathbb{R}$: tout intervalle ouvert (non vide) de $\mathbb{R}$ contient une infinité d'irrationnels.

Démonstration

On commence par remarquer que tout intervalle ouvert non vide de $\mathbb{R}$ contient un intervalle du type $]a,b[$. On peut donc supposer que $I =]a,b[$ par la suite.

1. *Tout intervalle contient un rationnel.*

   On commence par montrer l'affirmation :

$$\forall a,b \in \mathbb{R} \ \ (a < b \implies \exists r \in \mathbb{Q} \mid a < r < b) \tag{6.3}$$

   Donnons d'abord l'idée de la preuve. Trouver un tel rationnel $r = \frac{p}{q}$, avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, revient à trouver de tels entiers p et q vérifiant $qa < p < qb$. Cela revient à trouver un $q \in \mathbb{N}^*$ tel que l'intervalle ouvert $]qa, qb[$ contienne un entier p. Il suffit pour cela que la longueur $qb - qa = q(b-a)$ de l'intervalle dépasse strictement 1, ce qui équivaut à $q > \frac{1}{b-a}$.

Passons à la rédaction définitive. D'après la propriété d'Archimède (propriété $\mathbb{R}3$), il existe un entier q tel que $q > \frac{1}{b-a}$. Comme $b-a>0$, on a $q \in \mathbb{N}^*$. Posons $p = E(aq)+1$. Alors $p-1 \leqslant aq < p$. On en déduit d'une part $a < \frac{p}{q}$, et d'autre part $\frac{p}{q} - \frac{1}{q} \leqslant a$, donc $\frac{p}{q} \leqslant a + \frac{1}{q} < a + b - a = b$. Donc $\frac{p}{q} \in]a, b[$. On a montré l'affirmation (6.3).

2. *Tout intervalle contient un irrationnel.*

   Partant de a, b réels tels que $a < b$, on peut appliquer l'implication de l'affirmation (6.3) au couple $(a-\sqrt{2}, b-\sqrt{2})$. On en déduit qu'il existe un rationnel r dans l'intervalle $]a-\sqrt{2}, b-\sqrt{2}[$ et par translation $r+\sqrt{2} \in]a,b[$. Or $r+\sqrt{2}$ est irrationnel, car sinon comme les rationnels sont stables par somme, $\sqrt{2} = -r + r + \sqrt{2}$ serait rationnel, ce qui est faux d'après la proposition 38. On a donc montré que si $a < b$, l'intervalle $]a,b[$ contient aussi un irrationnel.

3. *Tout intervalle contient une infinité de rationnels et d'irrationnels.*

   On va déduire de l'existence d'un rationnel et d'un irrationnel dans tout intervalle $]a,b[$ le fait qu'il existe une infinité de chaque dans un tel intervalle ouvert. En effet pour un entier $N \geqslant 1$, on considère l'ensemble de N sous-intervalles ouverts :

$$\left]a, a+\frac{b-a}{N}\right[, \quad \left]a+\frac{b-a}{N}, a+\frac{2(b-a)}{N}\right[, \quad \ldots \quad \left]a+\frac{(N-1)(b-a)}{N}, b\right[.$$

   Chaque sous-intervalle contient un rationnel et un irrationnel, donc $]a,b[$ contient (au moins) N rationnels et N irrationnels. Comme ceci est vrai pour tout entier $N \geqslant 1$, l'intervalle ouvert $]a,b[$ contient alors une infinité de rationnels et une infinité d'irrationnels.

Mini-exercices

1. Montrer qu'une intersection d'intervalles est un intervalle. Qu'en est-il pour une réunion ? Trouver une condition nécessaire et suffisante afin que la réunion de deux intervalles soit un intervalle.
2. Montrer que l'ensemble des nombres décimaux (c'est-à-dire ceux de la forme $\frac{a}{10^n}$, avec $n \in \mathbb{N}$ et $a \in \mathbb{Z}$) est dense dans $\mathbb{R}$.
3. Construire un rationnel compris strictement entre 123 et 123,001. Ensuite construire un irrationnel. Sauriez-vous en construire une infinité ? Et entre π et $\pi + 0,001$?
4. Montrer que si $z = e^{i\alpha}$ et $z' = e^{i\beta}$ sont deux nombres complexes de module 1, avec $\alpha < \beta$, il existe un entier $n \in \mathbb{N}^*$ et une racine n-ième de l'unité $z = e^{i\gamma}$ avec $\alpha < \gamma < \beta$.

4. Borne supérieure

4.1. Maximum, minimum

Définition 34

Soit A une partie non vide de $\mathbb{R}$. Un réel α est un ***plus grand élément*** de A si :

$$\alpha \in A \text{ et } \forall x \in A \ \ x \leqslant \alpha.$$

S'il existe, le plus grand élément est unique, on le note alors $\max A$.

Le ***plus petit élément*** de A, noté $\min A$, s'il existe est le réel α tel que $\alpha \in A$ et $\forall x \in A \ \ x \geqslant \alpha$.

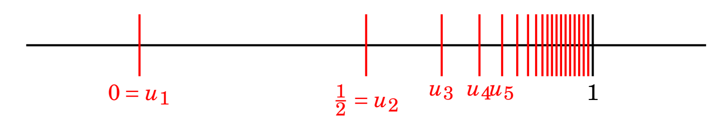
Le plus grand élément s'appelle aussi le ***maximum*** et le plus petit élément, le ***minimum***. Il faut garder à l'esprit que le plus grand élément ou le plus petit élément n'existent pas toujours.

Exemple 61

- $\max[a,b] = b$, $\min[a,b] = a$.
- L'intervalle $]a,b[$ n'a pas de plus grand élément, ni de plus petit élément.
- L'intervalle $[0,1[$ a pour plus petit élément 0 et n'a pas de plus grand élément.

Exemple 62

Soit $A = \left\{1 - \frac{1}{n} \mid n \in \mathbb{N}^*\right\}$.
Notons $u_n = 1 - \frac{1}{n}$ pour $n \in \mathbb{N}^*$. Alors $A = \left\{u_n \mid n \in \mathbb{N}^*\right\}$. Voici une représentation graphique de A sur la droite numérique :



1. A n'a pas de plus grand élément : Supposons qu'il existe un plus grand élément $\alpha = \max A$. On aurait alors $u_n \leqslant \alpha$, pour tout u_n. Ainsi $1 - \frac{1}{n} \leqslant \alpha$ donc $\alpha \geqslant 1 - \frac{1}{n}$. À la limite lorsque $n \to +\infty$ cela implique $\alpha \geqslant 1$. Comme α est le plus grand élément de A alors $\alpha \in A$. Donc il existe n_0 tel que $\alpha = u_{n_0}$. Mais alors $\alpha = 1 - \frac{1}{n_0} < 1$. Ce qui est en contradiction avec $\alpha \geqslant 1$. Donc A n'a pas de maximum.
2. $\min A = 0$: Il y a deux choses à vérifier tout d'abord pour $n = 1$, $u_1 = 0$ donc $0 \in A$. Ensuite pour tout $n \geqslant 1$, $u_n \geqslant 0$. Ainsi $\min A = 0$.

4.2. Majorants, minorants

Définition 35

Soit A une partie non vide de $\mathbb{R}$. Un réel M est un ***majorant*** de A si $\forall x \in A \ x \leqslant M$.
Un réel m est un ***minorant*** de A si $\forall x \in A \ x \geqslant m$.

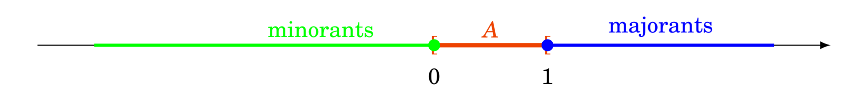
Exemple 63

- 3 est un majorant de $]0,2[$;
- $-7, -\pi, 0$ sont des minorants de $]0,+\infty[$ mais il n'y a pas de majorant.

Si un majorant (resp. un minorant) de A existe on dit que A est ***majorée*** (resp. ***minorée***).
Comme pour le minimum et maximum il n'existe pas toujours de majorant ni de minorant, en plus on n'a pas l'unicité.

Exemple 64

Soit $A = [0,1[$.



1. les majorants de A sont exactement les éléments de $[1,+\infty[$,
2. les minorants de A sont exactement les éléments de $]-\infty,0]$.

4.3. Borne supérieure, borne inférieure

Définition 36

Soit A une partie non vide de $\mathbb{R}$ et α un réel.

1. α est la ***borne supérieure*** de A si α est un majorant de A et si c'est le plus petit des majorants. S'il existe on le note $\sup A$.
2. α est la ***borne inférieure*** de A si α est un minorant de A et si c'est le plus grand des minorants. S'il existe on le note $\inf A$.

Exemple 65

- $\sup[a,b] = b$,
- $\inf[a,b] = a$,
- $\sup]a,b[= b$,
- $]0,+\infty[$ n'admet pas de borne supérieure,
- $\inf]0,+\infty[= 0$.

Exemple 66

Soit $A =]0,1]$.

1. $\sup A = 1$: en effet les majorants de A sont les éléments de $[1,+\infty[$. Donc le plus petit des majorants est 1.
2. $\inf A = 0$: les minorants sont les éléments de $]-\infty,0]$ donc le plus grand des minorants est 0.

Théorème 17. $\mathbb{R}$4

Toute partie de $\mathbb{R}$ non vide et majorée admet une borne supérieure.

De la même façon : Toute partie de $\mathbb{R}$ non vide et minorée admet une borne inférieure.

Remarque

C'est tout l'intérêt de la borne supérieure par rapport à la notion de plus grand élément, dès qu'une partie est bornée elle admet toujours une borne supérieure et une borne inférieure. Ce qui n'est pas le cas pour le plus grand ou plus petit élément. Gardez à l'esprit l'exemple $A = [0,1[$.

Proposition 41. Caractérisation de la borne supérieure

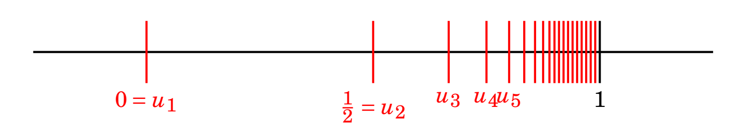
Soit A une partie non vide et majorée de $\mathbb{R}$. La borne supérieure de A est l'unique réel $\sup A$ tel que

(i) si $x \in A$, alors $x \leqslant \sup A$,

(ii) pour tout $y < \sup A$, il existe $x \in A$ tel que $y < x$.

Exemple 67

Reprenons l'exemple de la partie $A = \left\{1 - \frac{1}{n} \mid n \in \mathbb{N}^*\right\}$.



1. Nous avions vu que $\min A = 0$. Lorsque le plus petit élément d'une partie existe alors la borne inférieure vaut ce plus petit élément : donc $\inf A = \min A = 0$.
2. *Première méthode pour* $\sup A$. Montrons que $\sup A = 1$ en utilisant la définition de la borne supérieure. Soit M un majorant de A alors $M \geqslant 1 - \frac{1}{n}$, pour tout $n \geqslant 1$. Donc à la limite $M \geqslant 1$. Réciproquement si $M \geqslant 1$ alors M est un majorant de A. Donc les majorants sont les éléments de $[1, +\infty[$. Ainsi le plus petit des majorant est 1 et donc $\sup A = 1$.
3. *Deuxième méthode pour* $\sup A$. Montrons que $\sup A = 1$ en utilisant la caractérisation de la borne supérieure.
   (i) Si $x \in A$, alors $x \leqslant 1$ (1 est bien un majorant de A) ;
   (ii) pour tout $y < 1$, il existe $x \in A$ tel que $y < x$: en effet prenons n suffisamment grand tel que $0 < \frac{1}{n} < 1 - y$. Alors on a $y < 1 - \frac{1}{n} < 1$. Donc $x = 1 - \frac{1}{n} \in A$ convient.

   Par la caractérisation de la borne supérieure, $\sup A = 1$.

Démonstration

1. Montrons que $\sup A$ vérifie ces deux propriétés. La borne supérieure est en particulier un majorant, donc vérifie la première propriété. Pour la seconde, fixons $y < \sup A$. Comme $\sup A$ est le plus petit des majorants de A alors y n'est pas un majorant de A. Donc il existe $x \in A$ tel que $y < x$. Autrement dit $\sup A$ vérifie également la seconde propriété.
2. Montrons que réciproquement si un nombre α vérifie ces deux propriétés, il s'agit de $\sup A$. La première propriété montre que α est un majorant de A. Supposons par l'absurde que α n'est pas le plus petit des majorants. Il existe donc un autre majorant y de A vérifiant $y < \alpha$. La deuxième propriété montre l'existence d'un élément x de A tel que $y < x$, ce qui contredit le fait que y est un majorant de A. Cette contradiction montre donc que α est bien le plus petit des majorants de A, à savoir $\sup A$.

Remarques historiques

– Les propriétés $\mathbb{R}1$, $\mathbb{R}2$, $\mathbb{R}3$ et le théorème $\mathbb{R}4$ sont intrinsèques à la construction de $\mathbb{R}$ (que nous admettons).
– Il y a un grand saut entre $\mathbb{Q}$ et $\mathbb{R}$: on peut donner un sens précis à l'assertion « il y a beaucoup plus de nombres irrationnels que de nombres rationnels », bien que ces deux ensembles soient infinis, et même denses dans $\mathbb{R}$.
  D'autre part, la construction du corps des réels $\mathbb{R}$ est beaucoup plus récente que celle de $\mathbb{Q}$ dans l'histoire des mathématiques.
– La construction de $\mathbb{R}$ devient une nécessité après l'introduction du calcul infinitésimal (Newton et Leibniz vers 1670). Jusqu'alors l'existence d'une borne supérieure était considérée comme évidente et souvent confondue avec le plus grand élément.
– Ce n'est pourtant que beaucoup plus tard, dans les années 1860-1870 (donc assez récemment dans l'histoire des mathématiques) que deux constructions complètes de $\mathbb{R}$ sont données :

– Les coupures de Dedekind : $\mathscr{C}$ est une coupure si $\mathscr{C} \subset \mathbb{Q}$ et si $\forall r \in \mathscr{C}$ on a $r' < r \implies r' \in \mathscr{C}$.
– Le suites de Cauchy : ce sont les suites $(u_n)_{n\in\mathbb{N}}$ vérifiant la propriété

$$\forall \varepsilon > 0 \ \exists N \in \mathbb{N} \mid (m \geqslant N \ , n \geqslant N) \implies |u_m - u_n| \leqslant \varepsilon \ .$$

Les réels sont l'ensemble des suites de Cauchy (où l'on identifie deux suites de Cauchy dont la différence tend vers 0).

Mini-exercices

1. Soit A une partie de $\mathbb{R}$. On note $-A = \{-x | x \in A\}$. Montrer que $\min A = -\max(-A)$, c'est-à-dire que si l'une des deux quantités a un sens, l'autre aussi, et on a égalité.
2. Soit A une partie de $\mathbb{R}$. Montrer que A admet un plus petit élément si et seulement si A admet une borne inférieure qui appartient à A.
3. Même exercice, mais en remplaçant min par inf et max par sup.
4. Soit $A = \left\{(-1)^n \frac{n}{n+1} \mid n \in \mathbb{N}\right\}$. Déterminer, s'ils existent, le plus grand élément, le plus petit élément, les majorants, les minorants, la borne supérieure et la borne inférieure.
5. Même question avec $A = \left\{\frac{1}{1+x} \mid x \in [0, +\infty[\right\}$.

Auteurs

Arnaud Bodin
Niels Borne
Laura Desideri



7 Les suites

Vidéo ■ partie 1. Premières définitions
Vidéo ■ partie 2. Limite
Vidéo ■ partie 3. Exemples remarquables
Vidéo ■ partie 4. Théorèmes de convergence
Vidéo ■ partie 5. Suites récurrentes
Exercices ♦ Suites

Introduction

L'étude des suites numériques a pour objet la compréhension de l'évolution de séquences de nombres (réels, complexes ...). Ceci permet de modéliser de nombreux phénomènes de la vie quotidienne. Supposons par exemple que l'on place une somme S à un taux annuel de 10%. Si S_n représente la somme que l'on obtiendra après n années, on a

$$S_0 = S \quad S_1 = S \times 1,1 \quad \ldots \quad S_n = S \times (1,1)^n \ .$$

Au bout de $n = 10$ ans, on possédera donc $S_{10} = S_n = S \times (1,1)^{10} \approx S \times 2,59$: la somme de départ avec les intérêts cumulés.

1. Définitions

1.1. Définition d'une suite

Définition 37

- Une ***suite*** est une application $u : \mathbb{N} \to \mathbb{R}$.
- Pour $n \in \mathbb{N}$, on note $u(n)$ par u_n et on l'appelle n-ème ***terme*** ou ***terme général*** de la suite.

La suite est notée u, ou plus souvent $(u_n)_{n\in\mathbb{N}}$ ou simplement (u_n). Il arrive fréquemment que l'on considère des suites définies à partir d'un certain entier naturel n_0 plus grand que 0, on note alors $(u_n)_{n\geqslant n_0}$.

Exemple 68

- $(\sqrt{n})_{n\geqslant 0}$ est la suite de termes : 0, 1, $\sqrt{2}$, $\sqrt{3}$,...
- $((-1)^n)_{n\geqslant 0}$ est la suite qui alterne +1, −1, +1, −1,...
- La suite $(S_n)_{n\geqslant 0}$ de l'introduction définie par $S_n = S \times (1,1)^n$,
- $(F_n)_{n\geqslant 0}$ définie par $F_0 = 1$, $F_1 = 1$ et la relation $F_{n+2} = F_{n+1} + F_n$ pour $n \in \mathbb{N}$ (suite de Fibonacci). Les premiers termes sont 1, 1, 2, 3, 5, 8, 13, ... Chaque terme est la somme des deux précédents.
- $\left(\frac{1}{n^2}\right)_{n\geqslant 1}$. Les premiers termes sont 1, $\frac{1}{4}$, $\frac{1}{9}$, $\frac{1}{16}$, ...

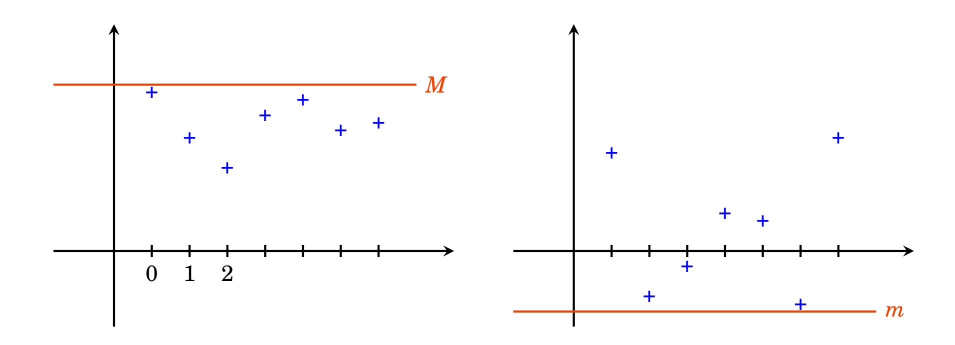
1.2. Suite majorée, minorée, bornée

Définition 38

Soit $(u_n)_{n\in\mathbb{N}}$ une suite.

- $(u_n)_{n\in\mathbb{N}}$ est ***majorée*** si $\exists M \in \mathbb{R} \quad \forall n \in \mathbb{N} \quad u_n \leqslant M$.
- $(u_n)_{n\in\mathbb{N}}$ est ***minorée*** si $\exists m \in \mathbb{R} \quad \forall n \in \mathbb{N} \quad u_n \geqslant m$.
- $(u_n)_{n\in\mathbb{N}}$ est ***bornée*** si elle est majorée et minorée, ce qui revient à dire :

$$\exists M \in \mathbb{R} \quad \forall n \in \mathbb{N} \quad |u_n| \leqslant M.$$



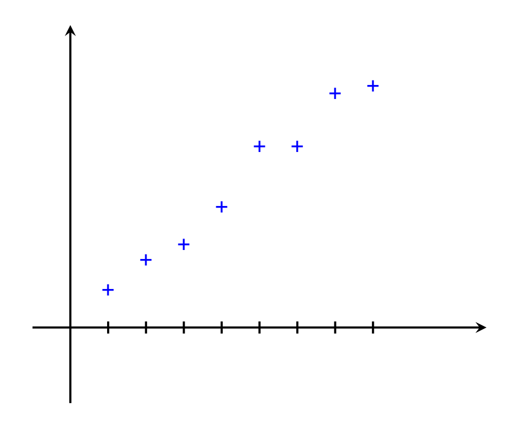
1.3. Suite croissante, décroissante

Définition 39

Soit $(u_n)_{n\in\mathbb{N}}$ une suite.

- $(u_n)_{n\in\mathbb{N}}$ est ***croissante*** si $\quad \forall n \in \mathbb{N} \quad u_{n+1} \geqslant u_n$.
- $(u_n)_{n\in\mathbb{N}}$ est ***strictement croissante*** si $\quad \forall n \in \mathbb{N} \quad u_{n+1} > u_n$.
- $(u_n)_{n\in\mathbb{N}}$ est ***décroissante*** si $\quad \forall n \in \mathbb{N} \quad u_{n+1} \leqslant u_n$.
- $(u_n)_{n\in\mathbb{N}}$ est ***strictement décroissante*** si $\quad \forall n \in \mathbb{N} \quad u_{n+1} < u_n$.
- $(u_n)_{n\in\mathbb{N}}$ est ***monotone*** si elle est croissante ou décroissante.
- $(u_n)_{n\in\mathbb{N}}$ est ***strictement monotone*** si elle est strictement croissante ou strictement décroissante.

Voici un exemple d'une suite croissante (mais pas strictement croissante) :

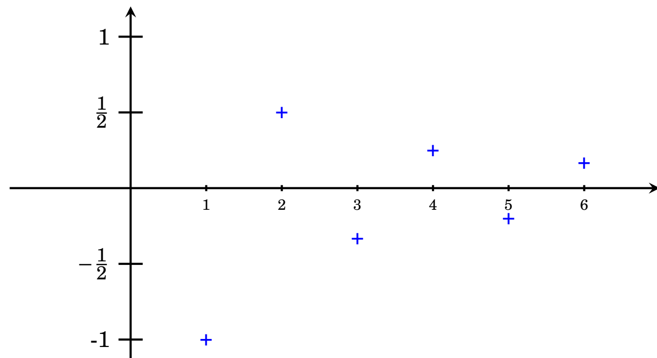


Remarque

- $(u_n)_{n\in\mathbb{N}}$ est croissante si et seulement si $\forall n \in \mathbb{N} \quad u_{n+1} - u_n \geqslant 0$.
- Si $(u_n)_{n\in\mathbb{N}}$ est une suite à termes strictement positifs, elle est croissante si et seulement si $\forall n \in \mathbb{N} \quad \frac{u_{n+1}}{u_n} \geqslant 1$.

Exemple 69

- La suite $(S_n)_{n\geqslant 0}$ de l'introduction est strictement croissante car $S_{n+1}/S_n = 1,1 > 1$.
- La suite $(u_n)_{n\geqslant 1}$ définie par $u_n = (-1)^n/n$ pour $n \geqslant 1$, n'est ni croissante ni décroissante. Elle est majorée par $1/2$ (borne atteinte en $n = 2$), minorée par -1 (borne atteinte en $n = 1$).



- La suite $\left(\frac{1}{n}\right)_{n\geqslant 1}$ est une suite strictement décroissante. Elle est majorée par 1 (borne atteinte pour $n = 1$), elle est minorée par 0 mais cette valeur n'est jamais atteinte.

Mini-exercices

1. La suite $\left(\frac{n}{n+1}\right)_{n\in\mathbb{N}}$ est-elle monotone ? Est-elle bornée ?
2. La suite $\left(\frac{n\sin(n!)}{1+n^2}\right)_{n\in\mathbb{N}}$ est-elle bornée ?
3. Réécrire les phrases suivantes en une phrase mathématique. Écrire ensuite la négation mathématique de chacune des phrases. (a) La suite $(u_n)_{n\in\mathbb{N}}$ est majorée par 7. (b) La suite $(u_n)_{n\in\mathbb{N}}$ est constante. (c) La suite $(u_n)_{n\in\mathbb{N}}$ est strictement positive à partir d'un certain rang. (d) $(u_n)_{n\in\mathbb{N}}$ n'est pas strictement croissante.
4. Est-il vrai qu'une suite croissante est minorée ? Majorée ?
5. Soit $x>0$ un réel. Montrer que la suite $\left(\frac{x^n}{n!}\right)_{n\in\mathbb{N}}$ est décroissante à partir d'un certain rang.

2. Limites

2.1. Introduction

Pour un trajet au prix normal de 20 euros on achète une carte d'abonnement de train à 50 euros et on obtient chaque billet à 10 euros. La publicité affirme « 50% de réduction ». Qu'en pensez-vous ?

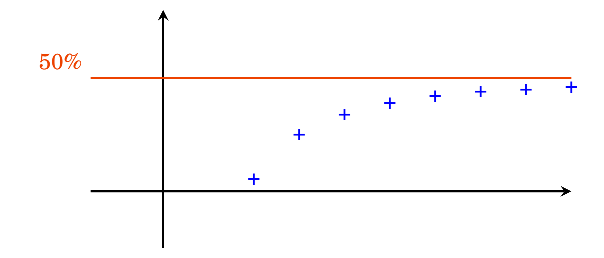
Pour modéliser la situation en termes de suites, on pose pour un entier $n \geqslant 1$:

$$u_n = 20n$$
$$v_n = 10n + 50$$

u_n est le prix payé au bout de n achats au tarif plein, et v_n celui au tarif réduit, y compris le prix de l'abonnement. La réduction est donc, en pourcentage :

$$1 - \frac{v_n}{u_n} = \frac{u_n - v_n}{u_n} = \frac{10n - 50}{20n} = 0,5 - \frac{5}{2n} \xrightarrow[n\to+\infty]{} 0,5$$

Il faut donc une infinité de trajets pour arriver à 50% de réduction !



2.2. Limite finie, limite infinie

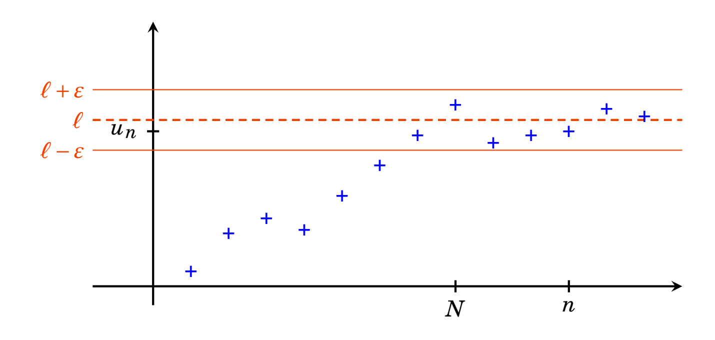
Soit $(u_n)_{n\in\mathbb{N}}$ une suite.

Définition 40

La suite $(u_n)_{n\in\mathbb{N}}$ a pour ***limite*** $\ell \in \mathbb{R}$ si : pour tout $\varepsilon > 0$, il existe un entier naturel N tel que si $n \geqslant N$ alors $|u_n - \ell| \leqslant \varepsilon$:

$$\boxed{\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \qquad (n \geqslant N \implies |u_n - \ell| \leqslant \varepsilon)}$$

On dit aussi que la suite $(u_n)_{n\in\mathbb{N}}$ ***tend vers*** ℓ. Autrement dit : u_n est proche d'aussi près que l'on veut de ℓ, à partir d'un certain rang.



Définition 41

1. La suite $(u_n)_{n\in\mathbb{N}}$ ***tend vers*** $+\infty$ si :

$$\forall A > 0 \quad \exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \qquad (n \geqslant N \implies u_n \geqslant A)$$

2. La suite $(u_n)_{n\in\mathbb{N}}$ ***tend vers*** $-\infty$ si :

$$\forall A > 0 \quad \exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \qquad (n \geqslant N \implies u_n \leqslant -A)$$

Remarque

1. On note $\lim_{n\to+\infty} u_n = \ell$ ou parfois $u_n \xrightarrow[n\to+\infty]{} \ell$, et de même pour une limite $\pm\infty$.
2. $\lim_{n\to+\infty} u_n = -\infty \iff \lim_{n\to+\infty} -u_n = +\infty$.
3. On raccourcit souvent la phrase logique en : $\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \qquad (n \geqslant N \implies |u_n - \ell| \leqslant \varepsilon)$. Noter que N dépend de ε et qu'on ne peut pas échanger l'ordre du « pour tout » et du « il existe ».
4. L'inégalité $|u_n - \ell| \leqslant \varepsilon$ signifie $\ell - \varepsilon \leqslant u_n \leqslant \ell + \varepsilon$. On aurait aussi pu définir la limite par la phrase : $\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \qquad (n \geqslant N \implies |u_n - \ell| < \varepsilon)$, où l'on a remplacé la dernière inégalité large par une inégalité stricte.

Définition 42

Une suite $(u_n)_{n\in\mathbb{N}}$ est ***convergente*** si elle admet une limite ***finie***. Elle est ***divergente*** sinon (c'est-à-dire soit la suite tend vers $\pm\infty$, soit elle n'admet pas de limite).

On va pouvoir parler de ***la*** limite, si elle existe, car il y a unicité de la limite :

Proposition 42

Si une suite est convergente, sa limite est unique.

Démonstration

On procède par l'absurde. Soit $(u_n)_{n\in\mathbb{N}}$ une suite convergente ayant deux limites $\ell \neq \ell'$. Choisissons $\varepsilon > 0$ tel que $\varepsilon < \frac{|\ell-\ell'|}{2}$.
Comme $\lim_{n\to+\infty} u_n = \ell$, il existe N_1 tel que $n \geqslant N_1$ implique $|u_n - \ell| < \varepsilon$.
De même $\lim_{n\to+\infty} u_n = \ell'$, il existe N_2 tel que $n \geqslant N_2$ implique $|u_n - \ell'| < \varepsilon$.
Notons $N = \max(N_1, N_2)$, on a alors pour ce N :

$$|u_N - \ell| < \varepsilon \quad \text{et} \quad |u_N - \ell'| < \varepsilon$$

Donc $|\ell - \ell'| = |\ell - u_N + u_N - \ell'| \leqslant |\ell - u_N| + |u_N - \ell'|$ d'après l'inégalité triangulaire. On en tire $|\ell - \ell'| \leqslant \varepsilon + \varepsilon = 2\varepsilon < |\ell - \ell'|$. On vient d'aboutir à l'inégalité $|\ell - \ell'| < |\ell - \ell'|$ qui est impossible. Bilan : notre hypothèse de départ est fausse et donc $\ell = \ell'$.

2.3. Propriétés des limites

Proposition 43

1. $\lim_{n\to+\infty} u_n = \ell \iff \lim_{n\to+\infty}(u_n - \ell) = 0 \iff \lim_{n\to+\infty}|u_n - \ell| = 0$,
2. $\lim_{n\to+\infty} u_n = \ell \implies \lim_{n\to+\infty}|u_n| = |\ell|$.

Démonstration

Cela résulte directement de la définition.

Proposition 44. Opérations sur les limites

Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites convergentes.

1. Si $\lim_{n\to+\infty} u_n = \ell$, où $\ell \in \mathbb{R}$, alors pour $\lambda \in \mathbb{R}$ on a $\lim_{n\to+\infty} \lambda u_n = \lambda\ell$.
2. Si $\lim_{n\to+\infty} u_n = \ell$ et $\lim_{n\to+\infty} v_n = \ell'$, où $\ell, \ell' \in \mathbb{R}$, alors

$$\lim_{n\to+\infty}(u_n + v_n) = \ell + \ell'$$
$$\lim_{n\to+\infty}(u_n \times v_n) = \ell \times \ell'$$

3. Si $\lim_{n\to+\infty} u_n = \ell$ où $\ell \in \mathbb{R}^* = \mathbb{R}\setminus\{0\}$ alors $u_n \neq 0$ pour n assez grand et $\lim_{n\to+\infty} \frac{1}{u_n} = \frac{1}{\ell}$.

Nous ferons la preuve dans la section suivante.
Nous utilisons continuellement ces propriétés, le plus souvent sans nous en rendre compte.

Exemple 70

Si $u_n \to \ell$ avec $\ell \neq \pm 1$, alors

$$u_n(1-3u_n) - \frac{1}{u_n^2 - 1} \xrightarrow[n\to+\infty]{} \ell(1-3\ell) - \frac{1}{\ell^2 - 1}.$$

Proposition 45. Opérations sur les limites infinies

Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites telles que $\lim_{n\to+\infty} v_n = +\infty$.

1. $\lim_{n\to+\infty} \frac{1}{v_n} = 0$
2. Si $(u_n)_{n\in\mathbb{N}}$ est minorée alors $\lim_{n\to+\infty}(u_n + v_n) = +\infty$
3. Si $(u_n)_{n\in\mathbb{N}}$ est minorée par un nombre $\lambda > 0$ alors $\lim_{n\to+\infty}(u_n \times v_n) = +\infty$
4. Si $\lim_{n\to+\infty} u_n = 0$ et $u_n > 0$ pour n assez grand alors $\lim_{n\to+\infty} \frac{1}{u_n} = +\infty$.

Exemple 71

Si (u_n) est la suite de terme général $\frac{1}{\sqrt{n}}$, alors $\lim_{n\to+\infty}(u_n) = 0$.

2.4. Des preuves !

Nous n'allons pas tout prouver mais seulement quelques résultats importants. Les autres se démontrent de manière tout à fait semblable.

Commençons par prouver un résultat assez facile (le premier point de la proposition 45) :

$$\text{« } \textit{Si} \quad \lim u_n = +\infty \quad \textit{alors} \quad \lim \frac{1}{u_n} = 0. \text{ »}$$

Démonstration

Fixons $\varepsilon > 0$. Comme $\lim_{n\to+\infty} u_n = +\infty$, il existe un entier naturel N tel que $n \geqslant N$ implique $u_n \geqslant \frac{1}{\varepsilon}$. On obtient alors $0 \leqslant \frac{1}{u_n} \leqslant \varepsilon$ pour $n \geqslant N$. On a donc montré que $\lim_{n\to+\infty} \frac{1}{u_n} = 0$.

Afin de prouver que la limite d'un produit est le produit des limites nous aurons besoin d'un peu de travail.

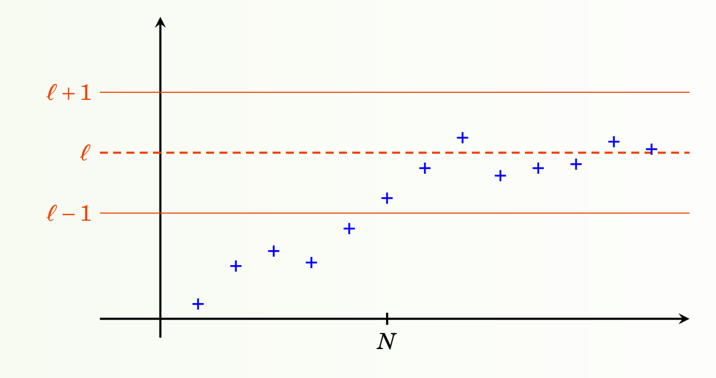
Proposition 46

Toute suite convergente est bornée.

Démonstration

Soit $(u_n)_{n\in\mathbb{N}}$ une suite convergeant vers le réel ℓ. En appliquant la définition de limite (définition 40) avec $\varepsilon = 1$, on obtient qu'il existe un entier naturel N tel que pour $n \geqslant N$ on ait $|u_n - \ell| \leqslant 1$, et donc pour $n \geqslant N$ on a

$$|u_n| = |\ell + (u_n - \ell)| \leqslant |\ell| + |u_n - \ell| \leqslant |\ell| + 1.$$



Donc si on pose

$$M = \max(|u_0|, |u_1|, \cdots, |u_{N-1}|, |\ell| + 1)$$

on a alors $\forall n \in \mathbb{N}\ |u_n| \leqslant M$.

Proposition 47

Si la suite $(u_n)_{n\in\mathbb{N}}$ est bornée et $\lim_{n\to+\infty} v_n = 0$ alors $\lim_{n\to+\infty}(u_n \times v_n) = 0$.

Exemple 72

Si $(u_n)_{n\geqslant 1}$ est la suite donnée par $u_n = \cos(n)$ et $(v_n)_{n\geqslant 1}$ est celle donnée par $v_n = \frac{1}{\sqrt{n}}$, alors $\lim_{n\to+\infty}(u_n v_n) = 0$.

Démonstration

La suite $(u_n)_{n\in\mathbb{N}}$ est bornée, on peut donc trouver un réel $M > 0$ tel que pour tout entier naturel n on ait $|u_n| \leqslant M$. Fixons $\varepsilon > 0$. On applique la définition de limite (définition 40) à la suite $(v_n)_{n\in\mathbb{N}}$ pour $\varepsilon' = \frac{\varepsilon}{M}$. Il existe donc un entier naturel N tel que $n \geqslant N$ implique $|v_n| \leqslant \varepsilon'$. Mais alors pour $n \geqslant N$ on a :

$$|u_n v_n| = |u_n||v_n| \leqslant M \times \varepsilon' = \varepsilon.$$

On a bien montré que $\lim_{n\to+\infty}(u_n \times v_n) = 0$.

Prouvons maintenant la formule concernant le produit de deux limites (voir proposition 44).

« *Si* $\lim u_n = \ell$ *et* $\lim v_n = \ell'$ *alors* $\lim u_n v_n = \ell\ell'$. »

Démonstration . Démonstration de la formule concernant le produit de deux limites

Le principe est d'écrire :

$$u_n v_n - \ell\ell' = (u_n - \ell)v_n + \ell(v_n - \ell')$$

D'après la proposition 47, la suite de terme général $\ell(v_n - \ell')$ tend vers 0. Par la même proposition il en est de même de la suite de terme général $(u_n - \ell)v_n$, car la suite convergente $(v_n)_{n\in\mathbb{N}}$ est bornée. On conclut que $\lim_{n\to+\infty}(u_n v_n - \ell\ell') = 0$, ce qui équivaut à $\lim_{n\to+\infty} u_n v_n = \ell\ell'$.

2.5. Formes indéterminées

Dans certaines situations, on ne peut rien dire à priori sur la limite, il faut faire une étude au cas par cas.

Exemple 73

1. « $+\infty - \infty$ » Cela signifie que si $u_n \to +\infty$ et $v_n \to -\infty$ il faut faire faire l'étude en fonction de chaque suite pour $\lim(u_n + v_n)$ comme le prouve les exemples suivants.

$$\lim_{n\to+\infty}\left(e^n - \ln(n)\right) = +\infty$$
$$\lim_{n\to+\infty}\left(n - n^2\right) = -\infty$$
$$\lim_{n\to+\infty}\left(\left(n + \frac{1}{n}\right) - n\right) = 0$$

2. « $0\times\infty$ »

$$\lim_{n\to+\infty}\frac{1}{\ln n}\times e^n=+\infty$$
$$\lim_{n\to+\infty}\frac{1}{n}\times\ln n=0$$
$$\lim_{n\to+\infty}\frac{1}{n}\times(n+1)=1$$

3. « $\frac{\infty}{\infty}$ », « $\frac{0}{0}$ », « 1^∞ », ...

2.6. Limite et inégalités

Proposition 48

1. Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites convergentes telles que : $\forall n\in\mathbb{N}$, $u_n\leqslant v_n$. Alors

$$\lim_{n\to+\infty}u_n\leqslant\lim_{n\to+\infty}v_n$$

2. Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites telles que $\lim_{n\to+\infty}u_n=+\infty$ et $\forall n\in\mathbb{N}$, $v_n\geqslant u_n$. Alors $\lim_{n\to+\infty}v_n=+\infty$.
3. Théorème des « gendarmes » : si $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ et $(w_n)_{n\in\mathbb{N}}$ sont trois suites telles que

$$\forall n\in\mathbb{N}\quad u_n\leqslant v_n\leqslant w_n$$

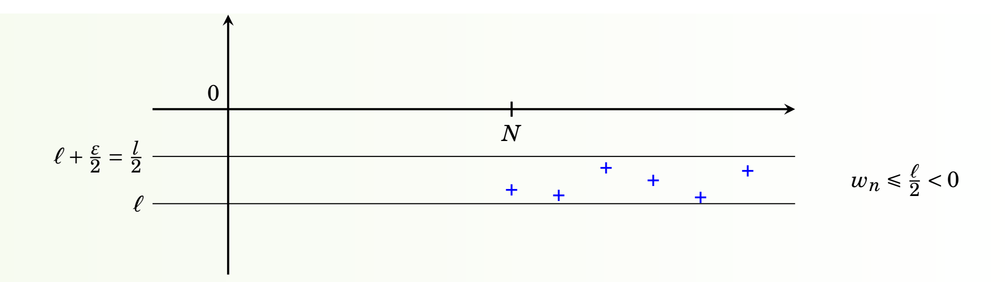
et $\lim_{n\to+\infty}u_n=\ell=\lim_{n\to+\infty}w_n$, alors la suite $(v_n)_{n\in\mathbb{N}}$ est convergente et $\lim_{n\to+\infty}v_n=\ell$.

Remarque

1. Soit $(u_n)_{n\in\mathbb{N}}$ une suite convergente telle que : $\forall n\in\mathbb{N}$, $u_n\geqslant 0$. Alors $\lim_{n\to+\infty}u_n\geqslant 0$.
2. Attention : si $(u_n)_{n\in\mathbb{N}}$ est une suite convergente telle que : $\forall n\in\mathbb{N}$, $u_n>0$, on ne peut affirmer que la limite est strictement positive mais seulement que $\lim_{n\to+\infty}u_n\geqslant 0$. Par exemple la suite $(u_n)_{n\in\mathbb{N}}$ donnée par $u_n=\frac{1}{n+1}$ est à termes strictement positifs, mais converge vers zéro.

Démonstration . Démonstration de la Proposition 48

1. En posant $w_n=v_n-u_n$, on se ramène à montrer que si une suite $(w_n)_{n\in\mathbb{N}}$ vérifie $\forall n\in\mathbb{N}$, $w_n\geqslant 0$ et converge, alors $\lim_{n\to+\infty}w_n\geqslant 0$. On procède par l'absurde en supposant que $\ell=\lim_{n\to+\infty}w_n<0$. En prenant $\varepsilon=|\frac{\ell}{2}|$ dans la définition de limite (définition 40), on obtient qu'il existe un entier naturel N tel que $n\geqslant N$ implique $|w_n-\ell|<\varepsilon=-\frac{\ell}{2}$. En particulier on a pour $n\geqslant N$ que $w_n<\ell-\frac{\ell}{2}=\frac{\ell}{2}<0$, une contradiction.



2. Laissé en exercice.
3. En soustrayant la suite $(u_n)_{n\in\mathbb{N}}$, on se ramène à montrer l'énoncé suivant : si $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont deux suites telles que : $\forall n \in \mathbb{N}, 0 \leqslant u_n \leqslant v_n$ et $\lim_{n\to+\infty} v_n = 0$, alors (u_n) converge et $\lim_{n\to+\infty} u_n = 0$. Soit $\varepsilon > 0$ et N un entier naturel tel que $n \geqslant N$ implique $|v_n| < \varepsilon$. Comme $|u_n| = u_n \leqslant v_n = |v_n|$, on a donc : $n \geqslant N$ implique $|u_n| < \varepsilon$. On a bien montré que $\lim_{n\to+\infty} u_n = 0$.

Exemple 74. Exemple d'application du théorème des « gendarmes »

Trouver la limite de la suite $(u_n)_{n\in\mathbb{N}}$ de terme général :

$$u_n = 2 + \frac{(-1)^n}{1+n+n^2}$$

Mini-exercices

1. Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_n = \frac{2n+1}{n+2}$. En utilisant la définition de la limite montrer que $\lim_{n\to+\infty} u_n = 2$. Trouver explicitement un rang à partir duquel $1,999 \leqslant u_n \leqslant 2,001$.
2. Déterminer la limite ℓ de la suite $(u_n)_{n\in\mathbb{N}}$ de terme général : $\frac{n+\cos n}{n-\sin n}$ et trouver un entier N tel que si $n \geqslant N$, on ait $|u_n - \ell| \leqslant 10^{-2}$.
3. La suite $(u_n)_{n\in\mathbb{N}}$ de terme général $(-1)^n e^n$ admet-elle une limite ? Et la suite de terme général $\frac{1}{u_n}$?
4. Déterminer la limite de la suite $(u_n)_{n\geqslant 1}$ de terme général $\sqrt{n+1} - \sqrt{n}$. Idem avec $v_n = \frac{\cos n}{\sin n + \ln n}$. Idem avec $w_n = \frac{n!}{n^n}$.

3. Exemples remarquables

3.1. Suite géométrique

Proposition 49. Suite géométrique

On fixe un réel a. Soit $(u_n)_{n\in\mathbb{N}}$ la suite de terme général : $u_n = a^n$.

1. Si $a = 1$, on a pour tout $n \in \mathbb{N}$: $u_n = 1$.
2. Si $a > 1$, alors $\lim_{n\to+\infty} u_n = +\infty$.
3. Si $-1 < a < 1$, alors $\lim_{n\to+\infty} u_n = 0$.
4. Si $a \leqslant -1$, la suite $(u_n)_{n\in\mathbb{N}}$ diverge.

Démonstration

1. est évident.
2. Écrivons $a = 1+b$ avec $b > 0$. Alors le binôme de Newton s'écrit $a^n = (1+b)^n = 1+nb+\binom{n}{2}b^2+\cdots+\binom{n}{k}b^k+\cdots+b^n$. Tous les termes sont positifs, donc pour tout entier naturel n on a : $a^n \geqslant 1+nb$. Or $\lim_{n\to+\infty}(1+nb) = +\infty$ car $b > 0$. On en déduit que $\lim_{n\to+\infty} a^n = +\infty$.
3. Si $a = 0$, le résultat est clair. Sinon, on pose $b = |\frac{1}{a}|$. Alors $b > 1$ et d'après le point précédent $\lim_{n\to+\infty} b^n = +\infty$. Comme pour tout entier naturel n on a : $|a|^n = \frac{1}{b^n}$, on en déduit que $\lim_{n\to+\infty}|a|^n = 0$, et donc aussi $\lim_{n\to+\infty} a^n = 0$.
4. Supposons par l'absurde que la suite $(u_n)_{n\in\mathbb{N}}$ converge vers le réel ℓ. De $a^2 \geqslant 1$, on déduit que pour tout entier naturel n, on a $a^{2n} \geqslant 1$. En passant à la limite, il vient $\ell \geqslant 1$. Comme de plus pour tout entier naturel n on a $a^{2n+1} \leqslant a \leqslant -1$, il vient en passant de nouveau à la limite $\ell \leqslant -1$. Mais comme on a déjà $\ell \geqslant 1$, on obtient une contradiction, et donc (u_n) ne converge pas.

3.2. Série géométrique

Proposition 50. Série géométrique

Soit a un réel, $a \neq 1$. En notant $\sum_{k=0}^{n} a^k = 1+a+a^2+\cdots+a^n$, on a :

$$\sum_{k=0}^{n} a^k = \frac{1-a^{n+1}}{1-a}$$

Démonstration

En multipliant par $1-a$ on fait apparaître une somme télescopique (presque tous les termes s'annulent) :

$$(1-a)\big(1+a+a^2+\cdots+a^n\big) = \big(1+a+a^2+\cdots+a^n\big) - \big(a+a^2+\cdots+a^{n+1}\big) = 1-a^{n+1}.$$

Remarque

Si $a \in]-1,1[$ et $(u_n)_{n\in\mathbb{N}}$ est la suite de terme général : $u_n = \sum_{k=0}^{n} a^k$, alors $\lim_{n\to+\infty} u_n = \frac{1}{1-a}$. De manière plus frappante, on peut écrire :

$$1+a+a^2+a^3+\cdots = \frac{1}{1-a}$$

Enfin, ces formules sont aussi valables si $a \in \mathbb{C}\setminus\{1\}$. Si $a = 1$, alors $1+a+a^2+\cdots+a^n = n+1$.

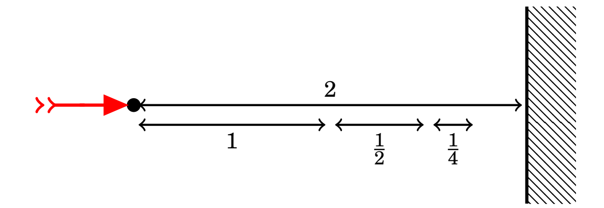
Exemple 75

L'exemple précédent avec $a = \frac{1}{2}$ donne

$$1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots = 2.$$

Cette formule était difficilement concevable avant l'avènement du calcul infinitésimal et a été popularisée sous le nom du ***paradoxe de Zénon***. On tire une flèche à 2 mètres d'une cible. Elle met un certain laps de temps pour parcourir la moitié de la distance, à savoir un mètre. Puis il lui faut encore du temps pour parcourir la moitié de la distance restante, et de nouveau

un certain temps pour la moitié de la distance encore restante. On ajoute ainsi une infinité de durées non nulles, et Zénon en conclut que la flèche n'atteint jamais sa cible !
L'explication est bien donnée par l'égalité ci-dessus : la somme d'une infinité de termes peut bien être une valeur finie !! Par exemple si la flèche va à une vitesse de 1 m/s, alors elle parcoure la première moitié en 1 s, le moitié de la distance restante en $\frac{1}{2}$ s, etc. Elle parcoure bien toute la distance en $1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots=2$ secondes !



3.3. Suites telles que $\left|\frac{u_{n+1}}{u_n}\right|<\ell<1$

Théorème 18

Soit $(u_n)_{n\in\mathbb{N}}$ une suite de réels non nuls. On suppose qu'il existe un réel ℓ tel que pour tout entier naturel n (ou seulement à partir d'un certain rang) on ait :

$$\left|\frac{u_{n+1}}{u_n}\right|<\ell<1.$$

Alors $\lim_{n\to+\infty} u_n=0$.

Démonstration

On suppose que la propriété $\left|\frac{u_{n+1}}{u_n}\right|<\ell<1$ est vraie pour tout entier naturel n (la preuve dans le cas où cette propriété n'est vraie qu'à partir d'un certain rang n'est pas très différente). On écrit

$$\frac{u_n}{u_0}=\frac{u_1}{u_0}\times\frac{u_2}{u_1}\times\frac{u_3}{u_2}\times\cdots\times\frac{u_n}{u_{n-1}}$$

ce dont on déduit

$$\left|\frac{u_n}{u_0}\right|<\ell\times\ell\times\ell\times\cdots\times\times\ell=\ell^n$$

et donc $|u_n|<|u_0|\ell^n$. Comme $\ell<1$, on a $\lim_{n\to+\infty}\ell^n=0$. On conclut que $\lim_{n\to+\infty}u_n=0$.

Corollaire 9

Soit $(u_n)_{n\in\mathbb{N}}$ une suite de réels non nuls.

Si $\lim_{n\to+\infty}\frac{u_{n+1}}{u_n}=0$, alors $\lim_{n\to+\infty}u_n=0$.

Exemple 76

Soit $a\in\mathbb{R}$. Alors $\lim_{n\to+\infty}\frac{a^n}{n!}=0$.

Démonstration

Si $a = 0$, le résultat est évident. Supposons $a \neq 0$, et posons $u_n = \frac{a^n}{n!}$. Alors

$$\frac{u_{n+1}}{u_n} = \frac{a^{n+1}}{(n+1)!} \cdot \frac{n!}{a^n} = \frac{a}{n+1}.$$

Pour conclure, on peut ou bien directement utiliser le corollaire : comme $\lim \frac{u_{n+1}}{u_n} = 0$ (car a est fixe), on a $\lim u_n = 0$. Ou bien, comme $\frac{u_{n+1}}{u_n} = \frac{a}{n+1}$, on déduit par le théorème que pour $n \geqslant N > 2|a|$ on a :

$$\left|\frac{u_{n+1}}{u_n}\right| = \frac{|a|}{n+1} \leqslant \frac{|a|}{N+1} < \frac{|a|}{N} < \frac{1}{2} = \ell$$

et donc $\lim_{n\to+\infty} u_n = 0$.

Remarque

1. Avec les notations du théorème, si on a pour tout entier naturel n à partir d'un certain rang : $\left|\frac{u_{n+1}}{u_n}\right| > \ell > 1$, alors la suite $(u_n)_{n\in\mathbb{N}}$ diverge. En effet, il suffit d'appliquer le théorème à la suite de terme général $\frac{1}{|u_n|}$ pour voir que $\lim_{n\to+\infty} |u_n| = +\infty$.
2. Toujours avec les notations du théorème, si $\ell = 1$ on ne peut rien dire.

Exemple 77

Pour un nombre réel a, $a > 0$, calculer $\lim_{n\to+\infty} \sqrt[n]{a}$.
On va montrer que $\lim_{n\to+\infty} \sqrt[n]{a} = 1$. Si $a = 1$, c'est clair. Supposons $a > 1$. Écrivons $a = 1 + h$, avec $h > 0$. Comme

$$\left(1 + \frac{h}{n}\right)^n \geqslant 1 + n\frac{h}{n} = 1 + h = a$$

(voir la preuve de la proposition 49) on a en appliquant la fonction racine n-ième, $\sqrt[n]{\cdot}$:

$$1 + \frac{h}{n} \geqslant \sqrt[n]{a} \geqslant 1.$$

On peut conclure grâce au théorème « des gendarmes » que $\lim_{n\to+\infty} \sqrt[n]{a} = 1$. Enfin, si $a < 1$, on applique le cas précédent à $b = \frac{1}{a} > 1$.

3.4. Approximation des réels par des décimaux

Proposition 51

Soit $a \in \mathbb{R}$. Posons

$$u_n = \frac{E(10^n a)}{10^n}.$$

Alors u_n est une approximation décimale de a à 10^{-n} près, en particulier $\lim_{n\to+\infty} u_n = a$.

Exemple 78

$\pi = 3,14159265\ldots$

$$u_0 = \frac{E(10^0\pi)}{10^0} = E(\pi) = 3$$
$$u_1 = \frac{E(10^1\pi)}{10^1} = \frac{E(31{,}415...)}{10} = 3,1$$
$$u_2 = \frac{E(10^2\pi)}{10^2} = \frac{E(314{,}15...)}{100} = 3,14$$
$$u_3 = 3,141$$

Démonstration

D'après la définition de la partie entière, on a

$$E(10^n a) \leqslant 10^n a < E(10^n a) + 1$$

donc

$$u_n \leqslant a < u_n + \frac{1}{10^n}$$

ou encore

$$0 \leqslant a - u_n < \frac{1}{10^n}.$$

Or la suite de terme général $\frac{1}{10^n}$ est une suite géométrique de raison $\frac{1}{10}$, donc elle tend vers 0. On en déduit que $\lim_{n\to+\infty} u_n = a$.

Exercice 4

Montrer que la suite $(u_n)_{n\in\mathbb{N}}$ de la proposition 51 est croissante.

Remarque

1. Les u_n sont des nombres décimaux, en particulier ce sont des nombres rationnels.
2. Ceci fournit une démonstration de la densité de $\mathbb{Q}$ dans $\mathbb{R}$. Pour $\varepsilon > 0$, et $I =]a-\varepsilon, a+\varepsilon[$, alors pour n assez grand, $u_n \in I \cap \mathbb{Q}$.

Mini-exercices

1. Déterminer la limite de la suite $(u_n)_{n\in\mathbb{N}}$ de terme général $5^n - 4^n$.
2. Soit $v_n = 1 + a + a^2 + \cdots + a^n$. Pour quelle valeur de $a \in \mathbb{R}$ la suite $(v_n)_{n\geqslant 1}$ a pour limite 3 (lorsque $n \to +\infty$) ?
3. Calculer la limite de $\frac{1+2+2^2+\cdots+2^n}{2^n}$.
4. Montrer que la somme des racines n-ièmes de l'unité est nulle.
5. Montrer que si $\sin(\frac{\theta}{2}) \neq 0$ alors $\frac{1}{2} + \cos(\theta) + \cos(2\theta) + \cdots + \cos(n\theta) = \frac{\sin((n+\frac{1}{2})\theta)}{2\sin(\frac{\theta}{2})}$ (penser à $e^{i\theta}$).
6. Soit $(u_n)_{n\geqslant 2}$ la suite de terme général $u_n = \ln(1+\frac{1}{2}) \times \ln(1+\frac{1}{3}) \times \cdots \times \ln(1+\frac{1}{n})$. Déterminer la limite de $\frac{u_{n+1}}{u_n}$. Que peut-on en déduire ?
7. Déterminer la limite de $\frac{\pi^n}{1\times 3\times 5\times\cdots\times(2n+1)}$ (où $\pi = 3,14\ldots$).
8. Soit a un réel. Montrer que pour tout $\varepsilon > 0$ il existe un couple $(m,n) \in \mathbb{Z} \times \mathbb{N}$ (et même une infinité) tel que $\left|a - \frac{m}{2^n}\right| \leqslant \varepsilon$.

4. Théorème de convergence

4.1. Toute suite convergente est bornée

Revenons sur une propriété importante que nous avons déjà démontrée dans la section sur les limites.

Proposition 52

Toute suite convergente est bornée.

La réciproque est fausse mais nous allons ajouter une hypothèse supplémentaire pour obtenir des résultats.

4.2. Suite monotone

Théorème 19

Toute suite croissante et majorée est convergente.

Remarque

Et aussi :
- Toute suite décroissante et minorée est convergente.
- Une suite croissante et qui n'est pas majorée tend vers $+\infty$.
- Une suite décroissante et qui n'est pas minorée tend vers $-\infty$.

Démonstration . Démonstration du théorème 19

Notons $A = \{u_n | n \in \mathbb{N}\} \subset \mathbb{R}$. Comme la suite $(u_n)_{n\in\mathbb{N}}$ est majorée, disons par le réel M, l'ensemble A est majoré par M, et de plus il est non vide. Donc d'après le théorème ℝ4 du chapitre sur les réels, l'ensemble A admet une borne supérieure : notons $\ell = \sup A$. Montrons que $\lim_{n\to+\infty} u_n = \ell$. Soit $\varepsilon > 0$. Par la caractérisation de la borne supérieure, il existe un élément u_N de A tel que $\ell - \varepsilon < u_N \leqslant \ell$. Mais alors pour $n \geqslant N$ on a $\ell - \varepsilon < u_N \leqslant u_n \leqslant \ell$, et donc $|u_n - \ell| \leqslant \varepsilon$.

4.3. Deux exemples

$\zeta(2)$

Soit $(u_n)_{n\geqslant1}$ la suite de terme général :

$$u_n = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2}.$$

- La suite $(u_n)_{n\geqslant1}$ est croissante : en effet $u_{n+1} - u_n = \frac{1}{(n+1)^2} > 0$.
- Montrons par récurrence que pour tout entier naturel $n \geqslant 1$ on a $u_n \leqslant 2 - \frac{1}{n}$.
  - Pour $n = 1$, on a $u_1 = 1 \leqslant 1 = 2 - \frac{1}{1}$.
  - Fixons $n \geqslant 1$ pour lequel on suppose $u_n \leqslant 2 - \frac{1}{n}$. Alors $u_{n+1} = u_n + \frac{1}{(n+1)^2} \leqslant 2 - \frac{1}{n} + \frac{1}{(n+1)^2}$. Or $\frac{1}{(n+1)^2} \leqslant \frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$, donc $u_{n+1} \leqslant 2 - \frac{1}{n+1}$, ce qui achève la récurrence.
- Donc la suite $(u_n)_{n\geqslant1}$ est croissante et majorée par 2 : elle converge.

Remarque

On note $\zeta(2)$ cette limite, vous montrerez plus tard qu'en fait $\zeta(2) = \frac{\pi^2}{6}$.

Suite harmonique

C'est la suite $(u_n)_{n\geqslant 1}$ de terme général :

$$u_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

Calculons $\lim_{n\to+\infty} u_n$.

- La suite $(u_n)_{n\geqslant 1}$ est croissante : en effet $u_{n+1} - u_n = \frac{1}{n+1} > 0$.
- Minoration de $u_{2^p} - u_{2^{p-1}}$. On a $u_2 - u_1 = 1 + \frac{1}{2} - 1 = \frac{1}{2}$; $u_4 - u_2 = \frac{1}{3} + \frac{1}{4} > \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$, et en général :
$$u_{2^p} - u_{2^{p-1}} = \underbrace{\frac{1}{2^{p-1}+1} + \frac{1}{2^{p-1}+2} + \cdots + \frac{1}{2^p}}_{2^{p-1}=2^p-2^{p-1} \text{ termes } \geqslant \frac{1}{2^p}} > 2^{p-1} \times \frac{1}{2^p} = \frac{1}{2}$$
- $\lim_{n\to+\infty} u_n = +\infty$. En effet
$$u_{2^p} - 1 = u_{2^p} - u_1 = (u_2 - u_1) + (u_4 - u_2) + \cdots + (u_{2^p} - u_{2^{p-1}}) \geqslant \frac{p}{2}$$
donc la suite $(u_n)_{n\geqslant 1}$ est croissante mais n'est pas bornée, donc elle tend vers $+\infty$.

4.4. Suites adjacentes

Définition 43

Les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont dites ***adjacentes*** si

1. $(u_n)_{n\in\mathbb{N}}$ est croissante et $(v_n)_{n\in\mathbb{N}}$ est décroissante,
2. pour tout $n \geqslant 0$, on a $u_n \leqslant v_n$,
3. $\lim_{n\to+\infty}(v_n - u_n) = 0$.

Théorème 20

Si les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont adjacentes, elles convergent vers la même limite.

Il y a donc deux résultats dans ce théorème, la convergence de (u_n) et (v_n) et en plus l'égalité des limites.

Les termes de la suites sont ordonnées ainsi :

$$u_0 \leqslant u_1 \leqslant u_2 \leqslant \cdots \leqslant u_n \leqslant \cdots\cdots \leqslant v_n \leqslant \cdots \leqslant v_2 \leqslant v_1 \leqslant v_0$$

Démonstration

- La suite $(u_n)_{n\in\mathbb{N}}$ est croissante et majorée par v_0, donc elle converge vers une limite ℓ.
- La suite $(v_n)_{n\in\mathbb{N}}$ est décroissante et minorée par u_0, donc elle converge vers une limite ℓ'.
- Donc $\ell' - \ell = \lim_{n\to+\infty}(v_n - u_n) = 0$, d'où $\ell' = \ell$.

Exemple 79

Reprenons l'exemple de $\zeta(2)$. Soient (u_n) et (v_n) les deux suites définies pour $n \geqslant 1$ par

$$u_n = \sum_{k=1}^{n} \frac{1}{k^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \quad \text{et} \quad v_n = u_n + \frac{2}{n+1}.$$

Montrons que (u_n) et (v_n) sont deux suites adjacentes :

1(a) (u_n) est croissante car $u_{n+1} - u_n = \frac{1}{(n+1)^2} > 0$.

(b) (v_n) est décroissante : $v_{n+1} - v_n = \frac{1}{(n+1)^2} + \frac{2}{n+2} - \frac{2}{n+1} = \frac{n+2+2(n+1)^2-2(n+1)(n+2)}{(n+2)(n+1)^2} = \frac{-n}{(n+2)(n+1)^2} < 0$

2. Pour tout $n \geqslant 1$: $v_n - u_n = \frac{2}{n+1} > 0$, donc $u_n \leqslant v_n$.

3. Enfin comme $v_n - u_n = \frac{2}{n+1}$ donc $\lim(v_n - u_n) = 0$.

Les suites (u_n) et (v_n) sont deux suites adjacentes, elles convergent donc vers une même limite finie ℓ. Nous avons en plus l'encadrement $u_n \leqslant \ell \leqslant v_n$ pour tout $n \geqslant 1$. Ceci fournit des approximations de la limite : par exemple pour $n = 3$, $1 + \frac{1}{4} + \frac{1}{9} \leqslant \ell \leqslant 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{2}$ donc $1,3611\ldots \leqslant \ell \leqslant 1,8611\ldots$

Exercice 5

Soit $(u_n)_{n\geqslant 1}$ la suite de terme général :

$$u_n = 1 + \frac{1}{2^3} + \frac{1}{3^3} + \cdots + \frac{1}{n^3}.$$

Montrer que la suite $(u_n)_{n\geqslant 1}$ converge (on pourra considérer la suite $(v_n)_{n\geqslant 1}$ de terme général $v_n = u_n + \frac{1}{n^2}$).

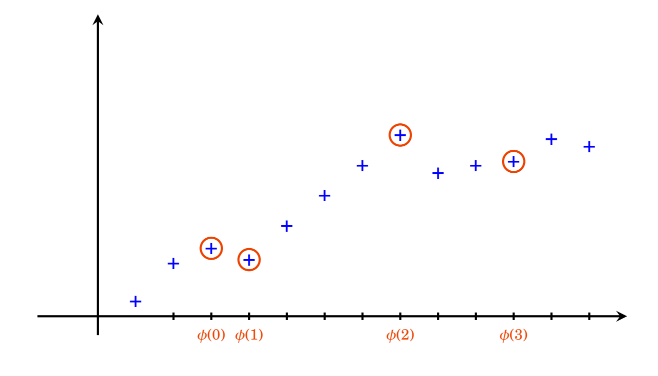
Remarque

On note $\zeta(3)$ cette limite. On l'appelle aussi constante d'Apéry. Roger Apéry a prouvé en 1978 que $\zeta(3) \notin \mathbb{Q}$.

4.5. Théorème de Bolzano-Weierstrass

Définition 44

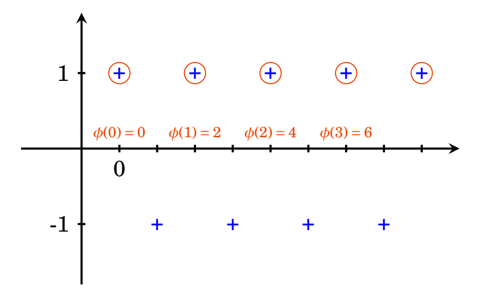
Soit $(u_n)_{n\in\mathbb{N}}$ une suite. Une ***suite extraite*** ou ***sous-suite*** de $(u_n)_{n\in\mathbb{N}}$ est une suite de la forme $(u_{\phi(n)})_{n\in\mathbb{N}}$, où $\phi : \mathbb{N} \to \mathbb{N}$ est une application strictement croissante.

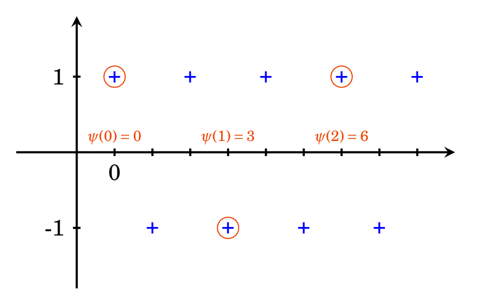


Exemple 80

Soit la suite $(u_n)_{n\in\mathbb{N}}$ de terme général $u_n = (-1)^n$.

- Si on considère $\phi : \mathbb{N} \to \mathbb{N}$ donnée par $\phi(n) = 2n$, alors la suite extraite correspondante a pour terme général $u_{\phi(n)} = (-1)^{2n} = 1$, donc la suite $(u_{\phi(n)})_{n\in\mathbb{N}}$ est constante égale à 1.
- Si on considère $\psi : \mathbb{N} \to \mathbb{N}$ donnée par $\psi(n) = 3n$, alors la suite extraite correspondante a pour terme général $u_{\psi(n)} = (-1)^{3n} = \left((-1)^3\right)^n = (-1)^n$. La suite $(u_{\psi(n)})_{n\in\mathbb{N}}$ est donc égale à $(u_n)_{n\in\mathbb{N}}$.





Proposition 53

Soit $(u_n)_{n\in\mathbb{N}}$ une suite. Si $\lim_{n\to+\infty} u_n = \ell$, alors pour toute suite extraite $(u_{\phi(n)})_{n\in\mathbb{N}}$ on a $\lim_{n\to+\infty} u_{\phi(n)} = \ell$.

Démonstration

Soit $\varepsilon > 0$. D'après la définition de limite (définition 40), il existe un entier naturel N tel que $n \geqslant N$ implique $|u_n - \ell| < \varepsilon$. Comme l'application ϕ est strictement croissante, on montre facilement par récurrence que pour tout n, on a $\phi(n) \geqslant n$. Ceci implique en particulier que si $n \geqslant N$, alors aussi $\phi(n) \geqslant N$, et donc $|u_{\phi(n)} - \ell| < \varepsilon$. Donc la définition de limite (définition 40) s'applique aussi à la suite extraite.

Corollaire 10

Soit $(u_n)_{n\in\mathbb{N}}$ une suite. Si elle admet une sous-suite divergente, ou bien si elle admet deux sous-suites convergeant vers des limites distinctes, alors elle diverge.

Exemple 81

Soit la suite $(u_n)_{n\in\mathbb{N}}$ de terme général $u_n = (-1)^n$. Alors $(u_{2n})_{n\in\mathbb{N}}$ converge vers 1, et $(u_{2n+1})_{n\in\mathbb{N}}$ converge vers -1 (en fait ces deux sous-suites sont constantes). On en déduit que la suite $(u_n)_{n\in\mathbb{N}}$ diverge.

Exercice 6

Soit $(u_n)_{n\in\mathbb{N}}$ une suite. On suppose que les deux sous-suites $(u_{2n})_{n\in\mathbb{N}}$ et $(u_{2n+1})_{n\in\mathbb{N}}$ convergent vers la même limite ℓ. Montrer que $(u_n)_{n\in\mathbb{N}}$ converge également vers ℓ.

Terminons par un résultat théorique très important.

Théorème 21. Théorème de Bolzano-Weierstrass

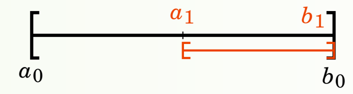
Toute suite bornée admet une sous-suite convergente.

Exemple 82

1. On considère la suite $(u_n)_{n\in\mathbb{N}}$ de terme général $u_n = (-1)^n$. Alors on peut considérer les deux sous-suites $(u_{2n})_{n\in\mathbb{N}}$ et $(u_{2n+1})_{n\in\mathbb{N}}$.
2. On considère la suite $(v_n)_{n\in\mathbb{N}}$ de terme général $v_n = \cos n$. Le théorème affirme qu'il existe une sous-suite convergente, mais il est moins facile de l'expliciter.

Démonstration . Démonstration du théorème 21

On procède par dichotomie. L'ensemble des valeurs de la suite est par hypothèse contenu dans un intervalle $[a,b]$. Posons $a_0 = a$, $b_0 = b$, $\phi(0) = 0$. Au moins l'un des deux intervalles $\left[a_0, \frac{a_0+b_0}{2}\right]$ ou $\left[\frac{a_0+b_0}{2}, b_0\right]$ contient u_n pour une infinité d'indices n. On note $[a_1,b_1]$ un tel intervalle, et on note $\phi(1)$ un entier $\phi(1) > \phi(0)$ tel que $u_{\phi(1)} \in [a_1,b_1]$.



En itérant cette construction, on construit pour tout entier naturel n un intervalle $[a_n,b_n]$, de longueur $\frac{b-a}{2^n}$, et un entier $\phi(n)$ tel que $u_{\phi(n)} \in [a_n,b_n]$. Notons que par construction la suite $(a_n)_{n\in\mathbb{N}}$ est croissante et la suite $(b_n)_{n\in\mathbb{N}}$ est décroissante.
Comme de plus $\lim_{n\to+\infty}(b_n - a_n) = \lim_{n\to+\infty} \frac{b-a}{2^n} = 0$, les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont adjacentes et donc convergent vers une même limite ℓ. On peut appliquer le théorème « des gendarmes » pour conclure que $\lim_{n\to+\infty} u_{\phi(n)} = \ell$.

Mini-exercices

1. Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_0 = 1$ et pour $n \geqslant 1$, $u_n = \sqrt{2+u_{n-1}}$. Montrer que cette suite est croissante et majorée par 2. Que peut-on en conclure ?
2. Soit $(u_n)_{n\geqslant 2}$ la suite définie par $u_n = \frac{\ln 4}{\ln 5} \times \frac{\ln 6}{\ln 7} \times \frac{\ln 8}{\ln 9} \times \cdots \times \frac{\ln(2n)}{\ln(2n+1)}$. Étudier la croissance de la suite. Montrer que la suite (u_n) converge.
3. Soit $N \geqslant 1$ un entier et $(u_n)_{n\in\mathbb{N}}$ la suite de terme général $u_n = \cos(\frac{n\pi}{N})$. Montrer que la suite diverge.
4. Montrer que les suites de terme général $u_n = \sum_{k=1}^{n} \frac{1}{k!}$ et $v_n = u_n + \frac{1}{n\cdot(n!)}$ sont adjacentes. Que peut-on en déduire ?
5. Soit $(u_n)_{n\geqslant 1}$ la suite de terme général $\sum_{k=1}^{n} \frac{(-1)^{k+1}}{k}$. On considère les deux suites extraites de terme général $v_n = u_{2n}$ et $w_n = u_{2n+1}$. Montrer que les deux suites $(v_n)_{n\geqslant 1}$ et $(w_n)_{n\geqslant 1}$ sont adjacentes. En déduire que la suite $(u_n)_{n\geqslant 1}$ converge.

6. Montrer qu'une suite bornée et divergente admet deux sous-suites convergeant vers des valeurs distinctes.

5. Suites récurrentes

Une catégorie essentielle de suites sont les suites récurrentes définies par une fonction. Ce chapitre est l'aboutissement de notre étude sur les suites, mais nécessite aussi l'étude de fonctions (voir «Limites et fonctions continues»).

5.1. Suite récurrente définie par une fonction

Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction. Une ***suite récurrente*** est définie par son premier terme et une relation permettant de calculer les termes de proche en proche :

$$u_0 \in \mathbb{R} \quad \text{et} \quad u_{n+1} = f(u_n) \quad \text{pour } n \geqslant 0$$

Une suite récurrente est donc définie par deux données : un terme initial u_0, et une relation de récurrence $u_{n+1} = f(u_n)$. La suite s'écrit ainsi :

$$u_0, \quad u_1 = f(u_0), \quad u_2 = f(u_1) = f(f(u_0)), \quad u_3 = f(u_2) = f(f(f(u_0))), \dots$$

Le comportement peut très vite devenir complexe.

Exemple 83

Soit $f(x) = 1 + \sqrt{x}$. Fixons $u_0 = 2$ et définissons pour $n \geqslant 0$: $u_{n+1} = f(u_n)$. C'est-à-dire $u_{n+1} = 1 + \sqrt{u_n}$. Alors les premiers termes de la suite sont :

$$2, \quad 1+\sqrt{2}, \quad 1+\sqrt{1+\sqrt{2}}, \quad 1+\sqrt{1+\sqrt{1+\sqrt{2}}}, \quad 1+\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{2}}}}, \dots$$

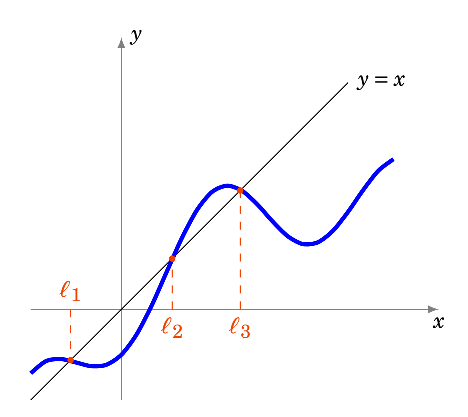
Voici un résultat essentiel concernant la limite si elle existe.

Proposition 54

Si f est une fonction continue et la suite récurrente (u_n) converge vers ℓ, alors ℓ est une solution de l'équation :

$$\boxed{f(\ell) = \ell}$$

Si on arrive à montrer que la limite existe alors cette proposition permet de calculer des candidats à être cette limite.



Une valeur ℓ, vérifiant $f(\ell) = \ell$ est un ***point fixe*** de f. La preuve est très simple et mérite d'être refaite à chaque fois.

Démonstration

Lorsque $n \to +\infty$, $u_n \to \ell$ et donc aussi $u_{n+1} \to \ell$. Comme $u_n \to \ell$ et que f est continue alors la suite $(f(u_n)) \to f(\ell)$. La relation $u_{n+1} = f(u_n)$ devient à la limite (lorsque $n \to +\infty$) : $\ell = f(\ell)$.

Nous allons étudier en détail deux cas particuliers fondamentaux : lorsque la fonction est croissante, puis lorsque la fonction est décroissante.

5.2. Cas d'une fonction croissante

Commençons par remarquer que pour une fonction croissante, le comportement de la suite (u_n) définie par récurrence est assez simple :

- Si $u_1 \geqslant u_0$ alors (u_n) est croissante.
- Si $u_1 \leqslant u_0$ alors (u_n) est décroissante.

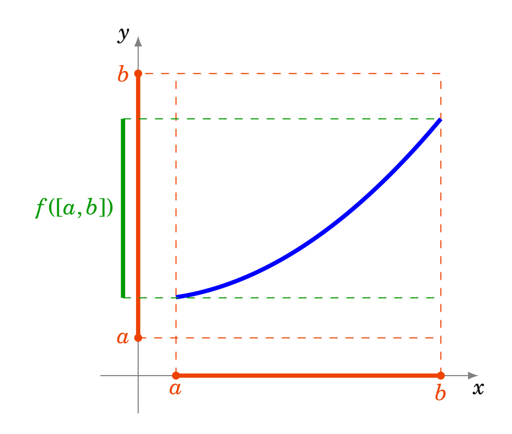
La preuve est une simple récurrence : par exemple si $u_1 \geqslant u_0$, alors comme f est croissante on a $u_2 = f(u_1) \geqslant f(u_0) = u_1$. Partant de $u_2 \geqslant u_1$ on en déduit $u_3 \geqslant u_2$,...

Voici le résultat principal :

Proposition 55

Si $f : [a, b] \to [a, b]$ une fonction continue et ***croissante***, alors quelque soit $u_0 \in [a, b]$, la suite récurrente (u_n) est monotone et converge vers $\ell \in [a, b]$ vérifiant $\boxed{f(\ell) = \ell}$.

Il y a une hypothèse importante qui est un peu cachée : f va de l'intervalle $[a, b]$ dans lui-même. Dans la pratique, pour appliquer cette proposition, il faut commencer par choisir $[a, b]$ et vérifier que $f([a, b]) \subset [a, b]$.



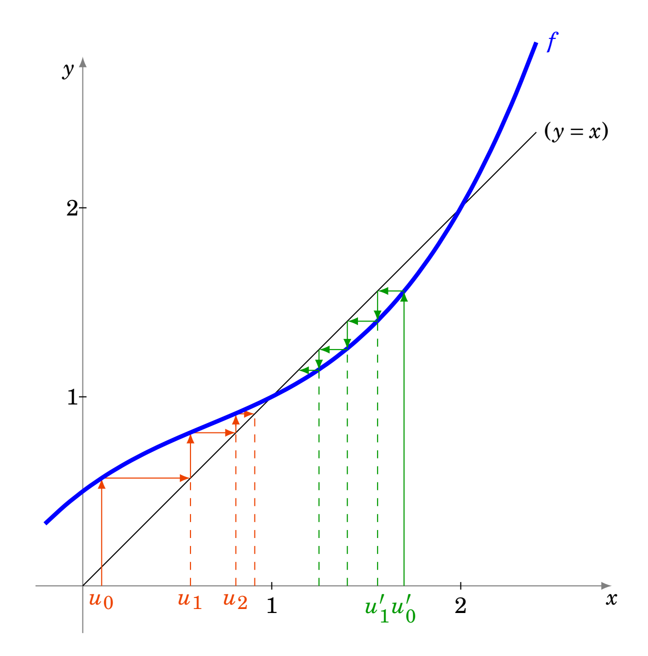
Démonstration

La preuve est une conséquence des résultats précédents. Par exemple si $u_1 \geqslant u_0$ alors la suite (u_n) est croissante, elle est majorée par b, donc elle converge vers un réel ℓ. Par la proposition 54, alors $f(\ell) = \ell$. Si $u_1 \leqslant u_0$, alors (u_n) est une décroissante et minorée par a, et la conclusion est la même.

Exemple 84

Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = \frac{1}{4}(x^2-1)(x-2)+x$ et $u_0 \in [0,2]$. Étudions la suite (u_n) définie par récurrence : $u_{n+1} = f(u_n)$ (pour tout $n \geqslant 0$).

1. Étude de f
   (a) f est continue sur $\mathbb{R}$.
   (b) f est dérivable sur $\mathbb{R}$ et $f'(x) > 0$.
   (c) Sur l'intervalle $[0,2]$, f est strictement croissante.
   (d) Et comme $f(0) = \frac{1}{2}$ et $f(2) = 2$ alors $f([0,2]) \subset [0,2]$.
2. Graphe de f



   Voici comment tracer la suite : on trace le graphe de f et la bissectrice $(y = x)$. On part d'une valeur u_0 (en rouge) sur l'axe des abscisses, la valeur $u_1 = f(u_0)$ se lit sur l'axe des ordonnées, mais on reporte la valeur de u_1 sur l'axe des abscisses par symétrie par rapport à la bissectrice. On recommence : $u_2 = f(u_1)$ se lit sur l'axe des ordonnées et on le reporte sur l'axe des abscisses, etc. On obtient ainsi une sorte d'escalier, et graphiquement on conjecture que la suite est croissante et tend vers 1. Si on part d'une autre valeur initiale u'_0 (en vert), c'est le même principe, mais cette fois on obtient un escalier qui descend.
3. Calcul des points fixes.
   Cherchons les valeurs x qui vérifient $(f(x) = x)$, autrement dit $(f(x) - x = 0)$, mais
   $$f(x) - x = \frac{1}{4}(x^2-1)(x-2) \tag{7.1}$$
   Donc les points fixes sont les $\{-1,1,2\}$. La limite de (u_n) est donc à chercher parmi ces 3 valeurs.
4. Premier cas : $u_0 = 1$ ou $u_0 = 2$.
   Alors $u_1 = f(u_0) = u_0$ et par récurrence la suite (u_n) est constante (et converge donc vers u_0).
5. Deuxième cas : $0 \leqslant u_0 < 1$.

– Comme $f([0,1]) \subset [0,1]$, la fonction f se restreint sur l'intervalle $[0,1]$ en une fonction $f : [0,1] \to [0,1]$.
– De plus sur $[0,1]$, $f(x) - x \geqslant 0$. Cela se déduit de l'étude de f ou directement de l'expression (7.1).
– Pour $u_0 \in [0,1[$, $u_1 = f(u_0) \geqslant u_0$ d'après le point précédent. Comme f est croissante, par récurrence, comme on l'a vu, la suite (u_n) est croissante.
– La suite (u_n) est croissante et majorée par 1, donc elle converge. Notons ℓ sa limite.
– D'une part ℓ doit être un point fixe de f : $f(\ell) = \ell$. Donc $\ell \in \{-1, 1, 2\}$.
– D'autre part la suite (u_n) étant croissante avec $u_0 \geqslant 0$ et majorée par 1, donc $\ell \in [0,1]$.
– Conclusion : si $0 \leqslant u_0 < 1$ alors (u_n) converge vers $\ell = 1$.

6. Troisième cas : $1 < u_0 < 2$.
La fonction f se restreint en $f : [1,2] \to [1,2]$. Sur l'intervalle $[1,2]$, f est croissante mais cette fois $f(x) \leqslant x$. Donc $u_1 \leqslant u_0$, et la suite (u_n) est décroissante. La suite (u_n) étant minorée par 1, elle converge. Si on note ℓ sa limite alors d'une part $f(\ell) = \ell$, donc $\ell \in \{-1, 1, 2\}$, et d'autre part $\ell \in [1, 2[$. Conclusion : (u_n) converge vers $\ell = 1$.

Le graphe de f joue un rôle très important, il faut le tracer même si on ne le demande pas explicitement. Il permet de se faire une idée très précise du comportement de la suite : Est-elle croissante ? Est-elle positive ? Semble-t-elle converger ? Vers quelle limite ? Ces indications sont essentielles pour savoir ce qu'il faut montrer lors de l'étude de la suite.

5.3. Cas d'une fonction décroissante

Proposition 56

Soit $f : [a,b] \to [a,b]$ une fonction continue et ***décroissante***. Soit $u_0 \in [a,b]$ et la suite récurrente (u_n) définie par $u_{n+1} = f(u_n)$. Alors :
– La sous-suite (u_{2n}) converge vers une limite ℓ vérifiant $f \circ f(\ell) = \ell$.
– La sous-suite (u_{2n+1}) converge vers une limite ℓ' vérifiant $f \circ f(\ell') = \ell'$.

Il se peut (ou pas !) que $\ell = \ell'$.

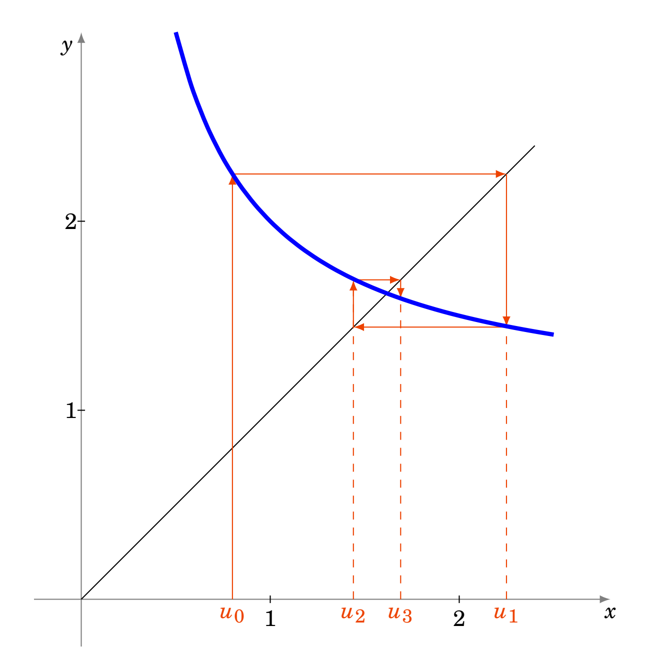
Démonstration

La preuve se déduit du cas croissant. La fonction f étant décroissante, la fonction $f \circ f$ est croissante. Et on applique la proposition 55 à la fonction $f \circ f$ et à la sous-suite (u_{2n}) définie par récurrence $u_2 = f \circ f(u_0)$, $u_4 = f \circ f(u_2)$,...
De même en partant de u_1 et $u_3 = f \circ f(u_1)$,...

Exemple 85

$$f(x) = 1 + \frac{1}{x}, \qquad u_0 > 0, \qquad u_{n+1} = f(u_n) = 1 + \frac{1}{u_n}$$

1. Étude de f. La fonction $f :]0, +\infty[\to]0, +\infty[$ est une fonction continue et strictement décroissante.
2. Graphe de f.



Le principe pour tracer la suite est le même qu'auparavant : on place u_0, on trace $u_1 = f(u_0)$ sur l'axe des ordonnées et on le reporte par symétrie sur l'axe des abscisses,... On obtient ainsi une sorte d'escargot, et graphiquement on conjecture que la suite converge vers le point fixe de f. En plus on note que la suite des termes de rang pair semble une suite croissante, alors que la suite des termes de rang impair semble décroissante.

3. Points fixes de $f \circ f$.

$$f \circ f(x) = f\big(f(x)\big) = f\Big(1+\frac{1}{x}\Big) = 1+\frac{1}{1+\frac{1}{x}} = 1+\frac{x}{x+1} = \frac{2x+1}{x+1}$$

Donc

$$f \circ f(x) = x \iff \frac{2x+1}{x+1} = x \iff x^2 - x - 1 = 0 \iff x \in \left\{\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\right\}$$

Comme la limite doit être positive, le seul point fixe à considérer est $\ell = \frac{1+\sqrt{5}}{2}$.
Attention ! Il y a un unique point fixe, mais on ne peut pas conclure à ce stade car f est définie sur $]0,+\infty[$ qui n'est pas un intervalle compact.

4. Premier cas $0 < u_0 \leqslant \ell = \frac{1+\sqrt{5}}{2}$.
Alors, $u_1 = f(u_0) \geqslant f(\ell) = \ell$; et par une étude de $f \circ f(x) - x$, on obtient que : $u_2 = f \circ f(u_0) \geqslant u_0$; $u_1 \geqslant f \circ f(u_1) = u_3$.
Comme $u_2 \geqslant u_0$ et $f \circ f$ est croissante, la suite (u_{2n}) est croissante. De même $u_3 \leqslant u_1$, donc la suite (u_{2n+1}) est décroissante. De plus comme $u_0 \leqslant u_1$, en appliquant f un nombre *pair* de fois, on obtient que $u_{2n} \leqslant u_{2n+1}$. La situation est donc la suivante :

$$u_0 \leqslant u_2 \leqslant \cdots \leqslant u_{2n} \leqslant \cdots \leqslant u_{2n+1} \leqslant \cdots \leqslant u_3 \leqslant u_1$$

La suite (u_{2n}) est croissante et majorée par u_1, donc elle converge. Sa limite ne peut être que l'unique point fixe de $f \circ f$: $\ell = \frac{1+\sqrt{5}}{2}$.
La suite (u_{2n+1}) est décroissante et minorée par u_0, donc elle converge aussi vers $\ell = \frac{1+\sqrt{5}}{2}$.
On en conclut que la suite (u_n) converge vers $\ell = \frac{1+\sqrt{5}}{2}$.

5. Deuxième cas $u_0 \geqslant \ell = \frac{1+\sqrt{5}}{2}$.
   On montre de la même façon que (u_{2n}) est décroissante et converge vers $\frac{1+\sqrt{5}}{2}$, et que (u_{2n+1}) est croissante et converge aussi vers $\frac{1+\sqrt{5}}{2}$.

Mini-exercices

1. Soit $f(x) = \frac{1}{9}x^3 + 1$, $u_0 = 0$ et pour $n \geqslant 0$: $u_{n+1} = f(u_n)$. Étudier en détails la suite (u_n) : (a) montrer que $u_n \geqslant 0$; (b) étudier et tracer le graphe de g ; (c) tracer les premiers termes de (u_n) ; (d) montrer que (u_n) est croissante ; (e) étudier la fonction $g(x) = f(x) - x$; (f) montrer que f admet deux points fixes sur $\mathbb{R}_+$, $0 < \ell < \ell'$; (g) montrer que $f([0,\ell]) \subset [0,\ell]$; (h) en déduire que (u_n) converge vers ℓ.
2. Soit $f(x) = 1 + \sqrt{x}$, $u_0 = 2$ et pour $n \geqslant 0$: $u_{n+1} = f(u_n)$. Étudier en détail la suite (u_n).
3. Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par : $u_0 \in [0,1]$ et $u_{n+1} = u_n - u_n^2$. Étudier en détail la suite (u_n).
4. Étudier la suite définie par $u_0 = 4$ et $u_{n+1} = \frac{4}{u_n+2}$.

Auteurs

Auteurs : Arnaud Bodin, Niels Borne, Laura Desideri
Dessins : Benjamin Boutin



8 Limites et fonctions continues

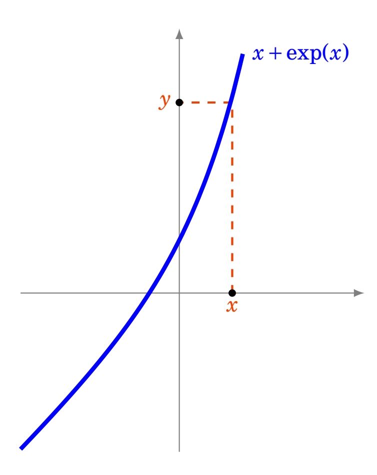
Vidéo ■ partie 1. Notions de fonction
Vidéo ■ partie 2. Limites
Vidéo ■ partie 3. Continuité en un point
Vidéo ■ partie 4. Continuité sur un intervalle
Vidéo ■ partie 5. Fonctions monotones et bijections
Exercices ♦ Limites de fonctions
Exercices ♦ Fonctions continues

Motivation

Nous savons résoudre beaucoup d'équations (par exemple $ax+b=0$, $ax^2+bx+c=0$,...) mais ces équations sont très particulières. Pour la plupart des équations nous ne saurons pas les résoudre, en fait il n'est pas évident de dire s'il existe une solution, ni combien il y en a. Considérons par exemple l'équation extrêmement simple :

$$x+\exp x=0$$

Il n'y a pas de formule connue (avec des sommes, des produits,... de fonctions usuelles) pour trouver la solution x.
Dans ce chapitre nous allons voir que grâce à l'étude de la fonction $f(x)=x+\exp x$ il est possible d'obtenir beaucoup d'informations sur la solution de l'équation $x+\exp x=0$ et même de l'équation plus générale $x+\exp x=y$ (où $y\in\mathbb{R}$ est fixé).



Nous serons capable de prouver que pour chaque $y\in\mathbb{R}$ l'équation « $x+\exp x=y$ » admet une solution x ; que cette solution est unique ; et nous saurons dire comment varie x en fonction de y. Le point

clé de tout cela est l'étude de la fonction f et en particulier de sa continuité. Même s'il n'est pas possible de trouver l'expression exacte de la solution x en fonction de y, nous allons mettre en place les outils théoriques qui permettent d'en trouver une solution approchée.

1. Notions de fonction

1.1. Définitions

Définition 45

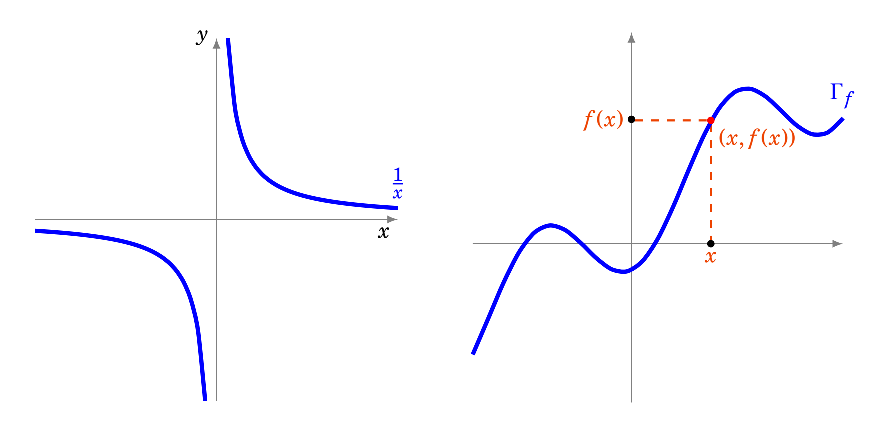
Une ***fonction*** d'une variable réelle à valeurs réelles est une application $f : U \to \mathbb{R}$, où U est une partie de $\mathbb{R}$. En général, U est un intervalle ou une réunion d'intervalles. On appelle U le ***domaine de définition*** de la fonction f.

Exemple 86

La fonction inverse :

$$\begin{array}{rcl} f :]-\infty,0[\cup]0,+\infty[& \longrightarrow & \mathbb{R} \\ x & \longmapsto & \dfrac{1}{x}. \end{array}$$

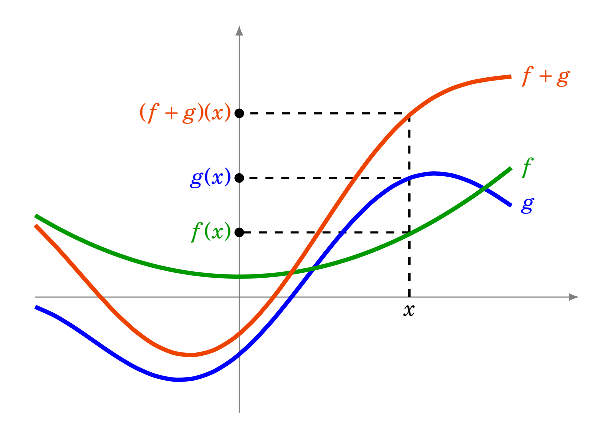
Le ***graphe*** d'une fonction $f : U \to \mathbb{R}$ est la partie Γ_f de $\mathbb{R}^2$ définie par $\Gamma_f = \{(x, f(x)) \mid x \in U\}$.



1.2. Opérations sur les fonctions

Soient $f : U \to \mathbb{R}$ et $g : U \to \mathbb{R}$ deux fonctions définies sur une même partie U de $\mathbb{R}$. On peut alors définir les fonctions suivantes :

- la ***somme*** de f et g est la fonction $f + g : U \to \mathbb{R}$ définie par $(f + g)(x) = f(x) + g(x)$ pour tout $x \in U$;
- le ***produit*** de f et g est la fonction $f \times g : U \to \mathbb{R}$ définie par $(f \times g)(x) = f(x) \times g(x)$ pour tout $x \in U$;
- la ***multiplication par un scalaire*** $\lambda \in \mathbb{R}$ de f est la fonction $\lambda \cdot f : U \to \mathbb{R}$ définie par $(\lambda \cdot f)(x) = \lambda \cdot f(x)$ pour tout $x \in U$.

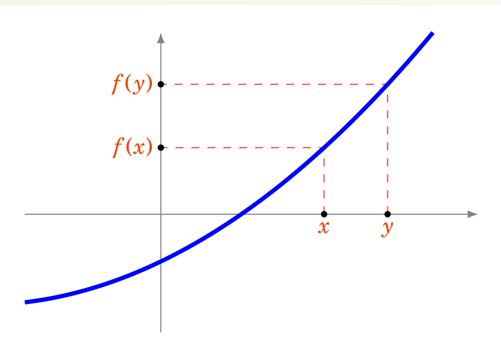


1.3. Fonctions majorées, minorées, bornées

Définition 46

Soient $f : U \to \mathbb{R}$ et $g : U \to \mathbb{R}$ deux fonctions. Alors :

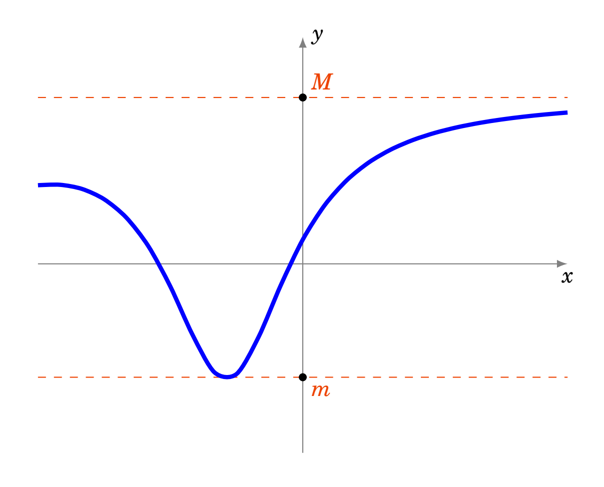
- $f \geqslant g$ si $\forall x \in U \; f(x) \geqslant g(x)$;
- $f \geqslant 0$ si $\forall x \in U \; f(x) \geqslant 0$;
- $f > 0$ si $\forall x \in U \; f(x) > 0$;
- f est dite ***constante*** sur U si $\exists a \in \mathbb{R} \; \forall x \in U \; f(x) = a$;
- f est dite ***nulle*** sur U si $\forall x \in U \; f(x) = 0$.



Définition 47

Soit $f : U \to \mathbb{R}$ une fonction. On dit que :

- f est ***majorée*** sur U si $\exists M \in \mathbb{R} \; \forall x \in U \; f(x) \leqslant M$;
- f est ***minorée*** sur U si $\exists m \in \mathbb{R} \; \forall x \in U \; f(x) \geqslant m$;
- f est ***bornée*** sur U si f est à la fois majorée et minorée sur U, c'est-à-dire si $\exists M \in \mathbb{R} \; \forall x \in U \; |f(x)| \leqslant M$.

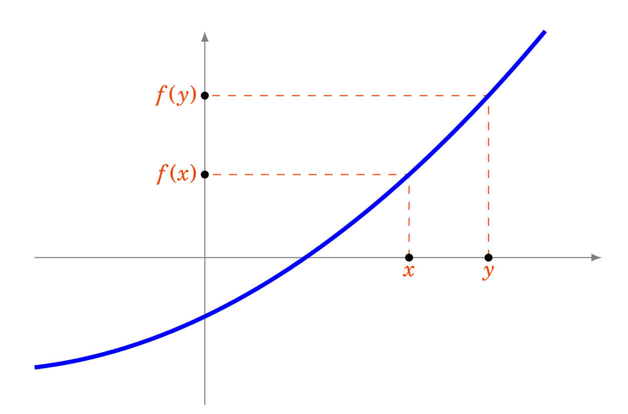


1.4. Fonctions croissantes, décroissantes

Définition 48

Soit $f : U \to \mathbb{R}$ une fonction. On dit que :

- f est ***croissante*** sur U si $\boxed{\forall x, y \in U \quad x \leqslant y \implies f(x) \leqslant f(y)}$
- f est ***strictement croissante*** sur U si $\forall x, y \in U \quad x < y \implies f(x) < f(y)$
- f est ***décroissante*** sur U si $\forall x, y \in U \quad x \leqslant y \implies f(x) \geqslant f(y)$
- f est ***strictement décroissante*** sur U si $\forall x, y \in U \quad x < y \implies f(x) > f(y)$
- f est ***monotone*** (resp. ***strictement monotone***) sur U si f est croissante ou décroissante (resp. strictement croissante ou strictement décroissante) sur U.



Exemple 87

- La fonction racine carrée $\begin{cases} [0, +\infty[\longrightarrow \mathbb{R} \\ x \longmapsto \sqrt{x} \end{cases}$ est strictement croissante.
- Les fonctions exponentielle $\exp : \mathbb{R} \to \mathbb{R}$ et logarithme $\ln :]0, +\infty[\to \mathbb{R}$ sont strictement croissantes.
- La fonction valeur absolue $\begin{cases} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto |x| \end{cases}$ n'est ni croissante, ni décroissante. Par contre, la fonction $\begin{cases} [0, +\infty[\longrightarrow \mathbb{R} \\ x \longmapsto |x| \end{cases}$ est strictement croissante.

1.5. Parité et périodicité

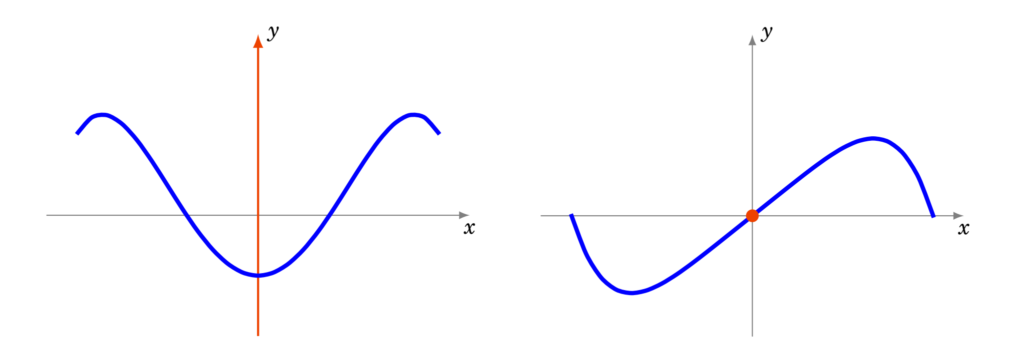
Définition 49

Soit I un intervalle de $\mathbb{R}$ symétrique par rapport à 0 (c'est-à-dire de la forme $]-a, a[$ ou $[-a, a]$ ou $\mathbb{R}$). Soit $f : I \to \mathbb{R}$ une fonction définie sur cet intervalle. On dit que :

- f est ***paire*** si $\forall x \in I \; f(-x) = f(x)$,
- f est ***impaire*** si $\forall x \in I \; f(-x) = -f(x)$.

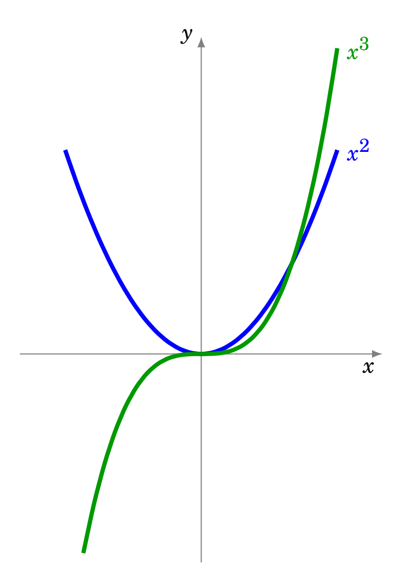
Interprétation graphique :

- f est paire si et seulement si son graphe est symétrique par rapport à l'axe des ordonnées.
- f est impaire si et seulement si son graphe est symétrique par rapport à l'origine.



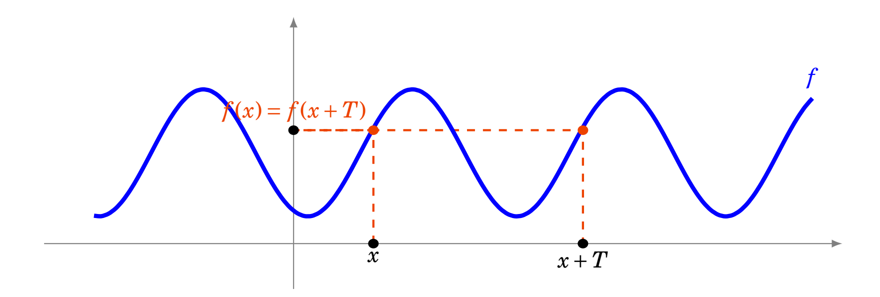
Exemple 88

- La fonction définie sur $\mathbb{R}$ par $x \mapsto x^{2n}$ ($n \in \mathbb{N}$) est paire.
- La fonction définie sur $\mathbb{R}$ par $x \mapsto x^{2n+1}$ ($n \in \mathbb{N}$) est impaire.
- La fonction $\cos : \mathbb{R} \to \mathbb{R}$ est paire. La fonction $\sin : \mathbb{R} \to \mathbb{R}$ est impaire.



Définition 50

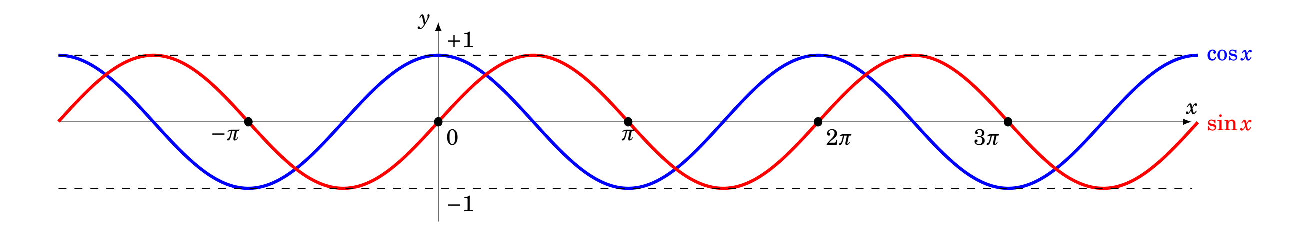
Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction et T un nombre réel, $T > 0$. La fonction f est dite ***périodique*** de période T si $\forall x \in \mathbb{R}\ f(x+T) = f(x)$.



Interprétation graphique : f est périodique de période T si et seulement si son graphe est invariant par la translation de vecteur $T\vec{i}$, où $\vec{i}$ est le premier vecteur de coordonnées.

Exemple 89

Les fonctions sinus et cosinus sont 2π-périodiques. La fonction tangente est π-périodique.



Mini-exercices

1. Soit $U =]-\infty, 0[$ et $f : U \to \mathbb{R}$ définie par $f(x) = 1/x$. f est-elle monotone ? Et sur $U =]0, +\infty[$? Et sur $U =]-\infty, 0[\cup]0, +\infty[$?
2. Pour deux fonctions paires que peut-on dire sur la parité de la somme ? du produit ? et de la composée ? Et pour deux fonctions impaires ? Et si l'une est paire et l'autre impaire ?
3. On note $\{x\} = x - E(x)$ la partie fractionnaire de x. Tracer le graphe de la fonction $x \mapsto \{x\}$ et montrer qu'elle est périodique.
4. Soit $f : \mathbb{R} \to \mathbb{R}$ la fonction définie par $f(x) = \frac{x}{1+x^2}$. Montrer que $|f|$ est majorée par $\frac{1}{2}$, étudier les variations de f (sans utiliser de dérivée) et tracer son graphe.
5. On considère la fonction $g : \mathbb{R} \to \mathbb{R}$, $g(x) = \sin\big(\pi f(x)\big)$, où f est définie à la question précédente. Déduire de l'étude de f les variations, la parité, la périodicité de g et tracer son graphe.

2. Limites

2.1. Définitions

Limite en un point

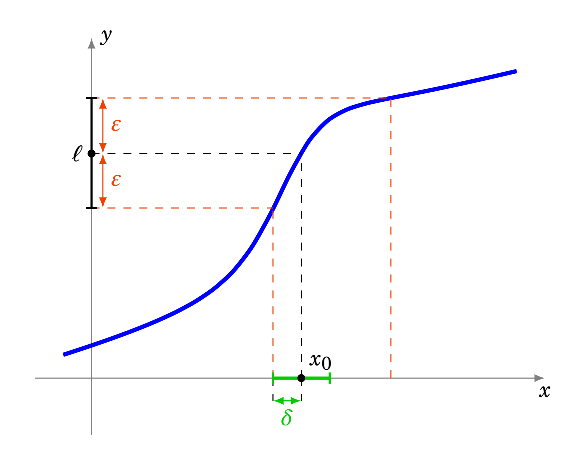
Soit $f : I \to \mathbb{R}$ une fonction définie sur un intervalle I de $\mathbb{R}$. Soit $x_0 \in \mathbb{R}$ un point de I ou une extrémité de I.

Définition 51

Soit $\ell \in \mathbb{R}$. On dit que ***f a pour limite ℓ en x_0*** si

$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad |x - x_0| < \delta \implies |f(x) - \ell| < \varepsilon$$

On dit aussi que ***$f(x)$ tend vers ℓ lorsque x tend vers x_0***. On note alors $\lim_{x \to x_0} f(x) = \ell$ ou bien $\lim_{x_0} f = \ell$.



Remarque

– L'inégalité $|x - x_0| < \delta$ équivaut à $x \in]x_0 - \delta, x_0 + \delta[$. L'inégalité $|f(x) - \ell| < \varepsilon$ équivaut à $f(x) \in]\ell - \varepsilon, \ell + \varepsilon[$.

– On peut remplacer certaines inégalités strictes « $<$ »par des inégalités larges « $\leqslant$ » dans la définition : $\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad |x - x_0| \leqslant \delta \implies |f(x) - \ell| \leqslant \varepsilon$

– Dans la définition de la limite

$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad |x - x_0| < \delta \implies |f(x) - \ell| < \varepsilon$$

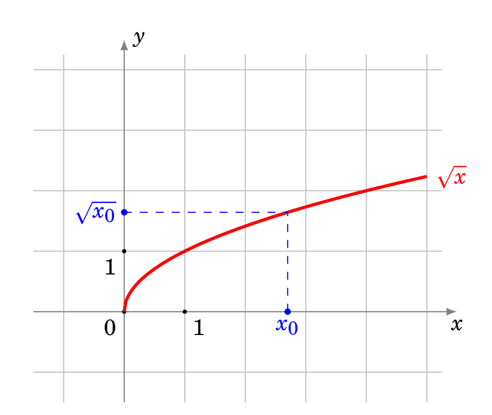
le quantificateur $\forall x \in I$ n'est là que pour être sûr que l'on puisse parler de $f(x)$. Il est souvent omis et l'existence de la limite s'écrit alors juste :

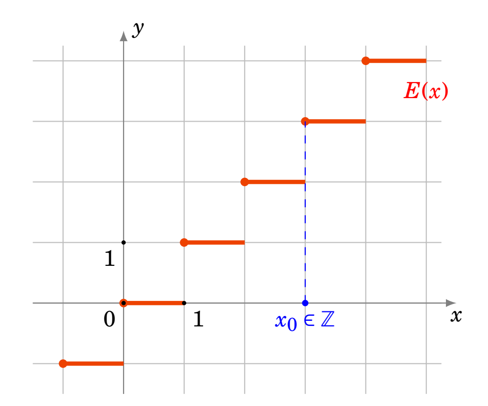
$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad |x - x_0| < \delta \implies |f(x) - \ell| < \varepsilon.$$

– N'oubliez pas que l'ordre des quantificateurs est important, on ne peut échanger le $\forall \varepsilon$ avec le $\exists \delta$: le δ dépend en général du ε. Pour marquer cette dépendance on peut écrire : $\forall \varepsilon > 0 \quad \exists \delta(\varepsilon) > 0 \ldots$

Exemple 90

- $\lim_{x \to x_0} \sqrt{x} = \sqrt{x_0}$ pour tout $x_0 \geqslant 0$,
- la fonction partie entière E n'a pas de limite aux points $x_0 \in \mathbb{Z}$.





Définition 52

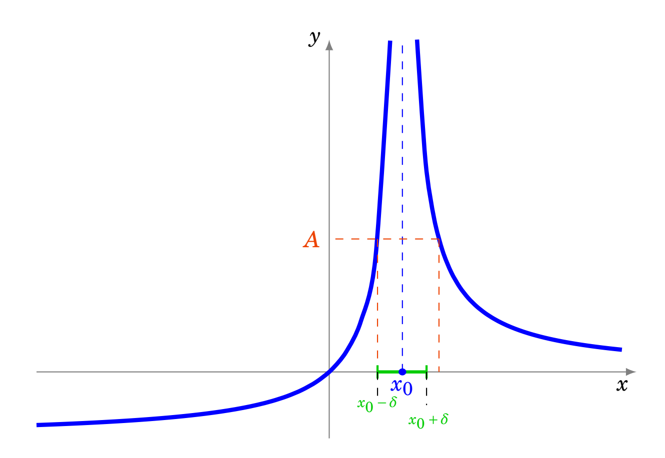
- On dit que ***f a pour limite*** $+\infty$ ***en*** x_0 si

$$\forall A > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad |x - x_0| < \delta \implies f(x) > A.$$

On note alors $\lim_{x \to x_0} f(x) = +\infty$.
- On dit que ***f a pour limite*** $-\infty$ ***en*** x_0 si

$$\forall A > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad |x - x_0| < \delta \implies f(x) < -A.$$

On note alors $\lim_{x \to x_0} f(x) = -\infty$.



Limite en l'infini

Soit $f : I \to \mathbb{R}$ une fonction définie sur un intervalle de la forme $I =]a, +\infty[$.

Définition 53

- Soit $\ell \in \mathbb{R}$. On dit que ***f a pour limite*** ℓ ***en*** $+\infty$ si

$$\forall \varepsilon > 0 \quad \exists B > 0 \quad \forall x \in I \quad x > B \implies |f(x) - \ell| < \varepsilon.$$

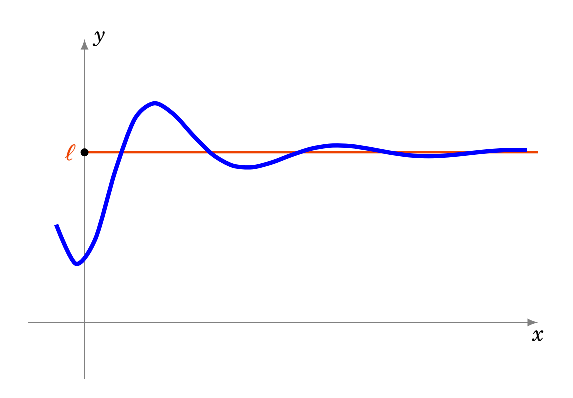
On note alors $\lim_{x \to +\infty} f(x) = \ell$ ou $\lim_{+\infty} f = \ell$.

– On dit que ***f a pour limite* $+\infty$ *en* $+\infty$** si

$$\forall A>0 \quad \exists B>0 \quad \forall x\in I \quad x>B \implies f(x)>A.$$

On note alors $\lim\limits_{x\to+\infty} f(x)=+\infty$.

On définit de la même manière la limite en $-\infty$ des fonctions définies sur les intervalles du type $]-\infty,a[$.



Exemple 91

On a les limites classiques suivantes pour tout $n\geqslant 1$:

– $\lim\limits_{x\to+\infty} x^n=+\infty$ et $\lim\limits_{x\to-\infty} x^n=\begin{cases}+\infty \text{ si } n \text{ est pair}\\ -\infty \text{ si } n \text{ est impair}\end{cases}$

– $\lim\limits_{x\to+\infty}\left(\frac{1}{x^n}\right)=0$ et $\lim\limits_{x\to-\infty}\left(\frac{1}{x^n}\right)=0$.

Exemple 92

Soit $P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ avec $a_n>0$ et $Q(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0$ avec $b_m>0$.

$$\lim_{x\to+\infty}\frac{P(x)}{Q(x)}=\begin{cases}+\infty & \text{si } n>m\\ \frac{a_n}{b_m} & \text{si } n=m\\ 0 & \text{si } n<m\end{cases}$$

Limite à gauche et à droite

Soit f une fonction définie sur un ensemble de la forme $]a,x_0[\cup]x_0,b[$.

Définition 54

– On appelle ***limite à droite*** en x_0 de f la limite de la fonction $f_{|]x_0,b[}$ en x_0 et on la note $\lim\limits_{x_0^+} f$.

– On définit de même la ***limite à gauche*** en x_0 de f : la limite de la fonction $f_{|]a,x_0[}$ en x_0 et on la note $\lim\limits_{x_0^-} f$.

– On note aussi $\lim_{\substack{x\to x_0\\ x>x_0}} f(x)$ pour la limite à droite et $\lim_{\substack{x\to x_0\\ x<x_0}} f(x)$ pour la limite à gauche.

Dire que $f : I \to \mathbb{R}$ admet une limite $\ell \in \mathbb{R}$ à droite en x_0 signifie donc :

$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad x_0 < x < x_0 + \delta \implies |f(x) - \ell| < \varepsilon.$$

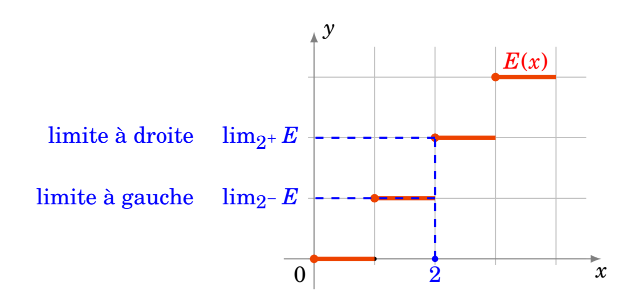
Si la fonction f a une limite en x_0, alors ses limites à gauche et à droite en x_0 coïncident et valent $\lim_{x_0} f$.
Réciproquement, si f a une limite à gauche et une limite à droite en x_0 et si ces limites valent $f(x_0)$ (si f est bien définie en x_0) alors f admet une limite en x_0.

Exemple 93

Considérons la fonction partie entière au point $x = 2$:

- comme pour tout $x \in]2,3[$ on a $E(x) = 2$, on a $\lim_{2^+} E = 2$,
- comme pour tout $x \in [1,2[$ on a $E(x) = 1$, on a $\lim_{2^-} E = 1$.

Ces deux limites étant différentes, on en déduit que E n'a pas de limite en 2.



2.2. Propriétés

Proposition 57

Si une fonction admet une limite, alors cette limite est unique.

On ne donne pas la démonstration de cette proposition, qui est très similaire à celle de l'unicité de la limite pour les suites (un raisonnement par l'absurde).

Soient deux fonctions f et g. On suppose que x_0 est un réel, ou que $x_0 = \pm\infty$.

Proposition 58

Si $\lim_{x_0} f = \ell \in \mathbb{R}$ et $\lim_{x_0} g = \ell' \in \mathbb{R}$, alors :

- $\lim_{x_0}(\lambda \cdot f) = \lambda \cdot \ell$ pour tout $\lambda \in \mathbb{R}$
- $\lim_{x_0}(f + g) = \ell + \ell'$
- $\lim_{x_0}(f \times g) = \ell \times \ell'$
- si $\ell \neq 0$, alors $\lim_{x_0} \frac{1}{f} = \frac{1}{\ell}$

De plus, si $\lim_{x_0} f = +\infty$ (ou $-\infty$) alors $\lim_{x_0} \frac{1}{f} = 0$.

Cette proposition se montre de manière similaire à la proposition analogue sur les limites de suites. Nous n'allons donc pas donner la démonstration de tous les résultats.

Démonstration

Montrons par exemple que si f tend en x_0 vers une limite ℓ non nulle, alors $\frac{1}{f}$ est bien définie dans un voisinage de x_0 et tend vers $\frac{1}{\ell}$.
Supposons $\ell > 0$, le cas $\ell < 0$ se montrerait de la même manière. Montrons tout d'abord que $\frac{1}{f}$ est bien définie et est bornée dans un voisinage de x_0 contenu dans I. Par hypothèse

$$\forall \varepsilon' > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad x_0 - \delta < x < x_0 + \delta \implies \ell - \varepsilon' < f(x) < \ell + \varepsilon'.$$

Si on choisit ε' tel que $0 < \varepsilon' < \ell/2$, alors on voit qu'il existe un intervalle $J = I \cap]x_0 - \delta, x_0 + \delta[$ tel que pour tout x dans J, $f(x) > \ell/2 > 0$, c'est-à-dire, en posant $M = \ell/2$:

$$\forall x \in J \quad 0 < \frac{1}{f(x)} < M.$$

Fixons à présent $\varepsilon > 0$. Pour tout $x \in J$, on a

$$\left|\frac{1}{f(x)} - \frac{1}{\ell}\right| = \frac{|\ell - f(x)|}{f(x)\ell} < \frac{M}{\ell}|\ell - f(x)|.$$

Donc, si dans la définition précédente de la limite de f en x_0 on choisit $\varepsilon' = \frac{\ell\varepsilon}{M}$, alors on trouve qu'il existe un $\delta > 0$ tel que

$$\forall x \in J \quad x_0 - \delta < x < x_0 + \delta \implies \left|\frac{1}{f(x)} - \frac{1}{\ell}\right| < \frac{M}{\ell}|\ell - f(x)| < \frac{M}{\ell}\varepsilon' = \varepsilon.$$

Proposition 59

Si $\lim_{x_0} f = \ell$ et $\lim_{\ell} g = \ell'$, alors $\lim_{x_0} g \circ f = \ell'$.

Ce sont des propriétés que l'on utilise sans s'en apercevoir !

Exemple 94

Soit $x \mapsto u(x)$ une fonction , $x_0 \in \mathbb{R}$ tel que $u(x) \to 2$ lorsque $x \to x_0$. Posons $f(x) = \sqrt{1 + \frac{1}{u(x)^2} + \ln u(x)}$. Si elle existe, quelle est la limite de f en x_0 ?

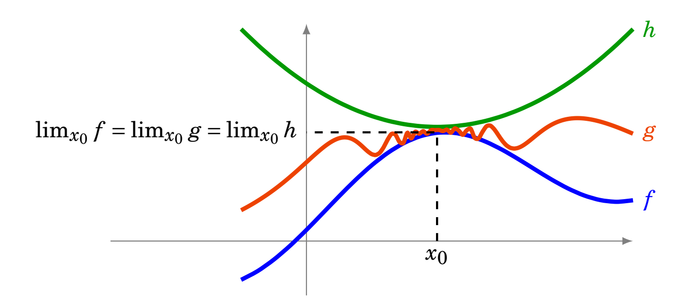
- Tout d'abord comme $u(x) \to 2$ alors $u(x)^2 \to 4$ donc $\frac{1}{u(x)^2} \to \frac{1}{4}$ (lorsque $x \to x_0$).
- De même comme $u(x) \to 2$ alors dans un voisinage de x_0 $u(x) > 0$ donc $\ln u(x)$ est bien définie dans ce voisinage et de plus $\ln u(x) \to \ln 2$ (lorsque $x \to x_0$).
- Cela entraîne que $1 + \frac{1}{u(x)^2} + \ln u(x) \to 1 + \frac{1}{4} + \ln 2$ lorsque $x \to x_0$. En particulier $1 + \frac{1}{u(x)^2} + \ln u(x) \geqslant 0$ dans un voisinage de x_0 donc $f(x)$ est bien définie dans un voisinage de x_0.
- Et par composition avec la racine carrée alors $f(x)$ a bien une limite en x_0 et $\lim_{x \to x_0} f(x) = \sqrt{1 + \frac{1}{4} + \ln 2}$.

Il y a des situations où l'on ne peut rien dire sur les limites. Par exemple si $\lim_{x_0} f = +\infty$ et $\lim_{x_0} g = -\infty$ alors on ne peut a priori rien dire sur la limite de $f + g$ (cela dépend vraiment de f et de g). On raccourci cela en $+\infty - \infty$ est une ***forme indéterminée***.
Voici une liste de formes indéterminées : $+\infty - \infty$; $0 \times \infty$; $\frac{\infty}{\infty}$; $\frac{0}{0}$; 1^∞ ; ∞^0.

Enfin voici une proposition très importante qui lie le comportement d'une limite avec les inégalités.

Proposition 60

- Si $f \leqslant g$ et si $\lim_{x_0} f = \ell \in \mathbb{R}$ et $\lim_{x_0} g = \ell' \in \mathbb{R}$, alors $\ell \leqslant \ell'$.
- Si $f \leqslant g$ et si $\lim_{x_0} f = +\infty$, alors $\lim_{x_0} g = +\infty$.
- Théorème des gendarmes
  Si $f \leqslant g \leqslant h$ et si $\lim_{x_0} f = \lim_{x_0} h = \ell \in \mathbb{R}$, alors g a une limite en x_0 et $\lim_{x_0} g = \ell$.



Mini-exercices

1. Déterminer, si elle existe, la limite de $\frac{2x^2-x-2}{3x^2+2x+2}$ en 0. Et en $+\infty$?
2. Déterminer, si elle existe, la limite de $\sin\left(\frac{1}{x}\right)$ en $+\infty$. Et pour $\frac{\cos x}{\sqrt{x}}$?
3. En utilisant la définition de la limite (avec des ε), montrer que $\lim_{x\to 2}(3x+1) = 7$.
4. Montrer que si f admet une limite finie en x_0 alors il existe $\delta > 0$ tel que f soit bornée sur $]x_0 - \delta, x_0 + \delta[$.
5. Déterminer, si elle existe, $\lim_{x\to 0} \frac{\sqrt{1+x}-\sqrt{1+x^2}}{x}$. Et $\lim_{x\to 2} \frac{x^2-4}{x^2-3x+2}$?

3. Continuité en un point

3.1. Définition

Soit I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$ une fonction.

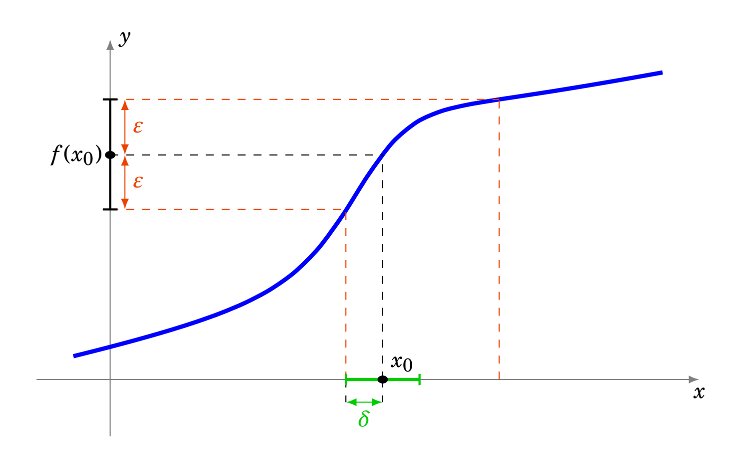
Définition 55

– On dit que f est ***continue en un point*** $x_0 \in I$ si

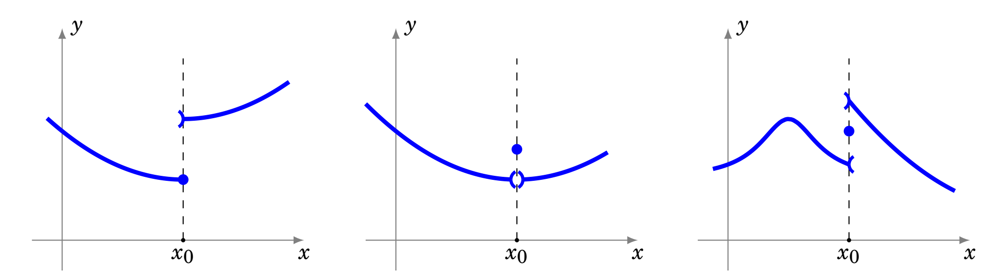
$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad |x - x_0| < \delta \implies |f(x) - f(x_0)| < \varepsilon$$

c'est-à-dire si f admet une limite en x_0 (cette limite vaut alors nécessairement $f(x_0)$).

– On dit que f est ***continue sur*** I si f est continue en tout point de I.



Intuitivement, une fonction est continue sur un intervalle, si on peut tracer son graphe « sans lever le crayon », c'est-à-dire si elle n'a pas de saut.
Voici des fonctions qui ne sont pas continues en x_0 :



Exemple 95

Les fonctions suivantes sont continues :

– une fonction constante sur un intervalle,
– la fonction racine carrée $x \mapsto \sqrt{x}$ sur $[0, +\infty[$,
– les fonctions sin et cos sur $\mathbb{R}$,
– la fonction valeur absolue $x \mapsto |x|$ sur $\mathbb{R}$,
– la fonction exp sur $\mathbb{R}$,
– la fonction ln sur $]0, +\infty[$.

Par contre, la fonction partie entière E n'est pas continue aux points $x_0 \in \mathbb{Z}$, puisqu'elle n'admet pas de limite en ces points. Pour $x_0 \in \mathbb{R} \setminus \mathbb{Z}$, elle est continue en x_0.

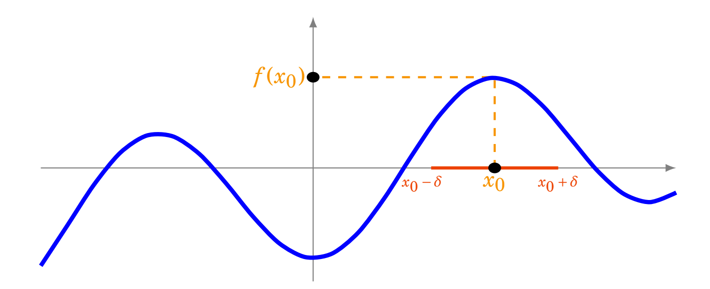
3.2. Propriétés

La continuité assure par exemple que si la fonction n'est pas nulle en un point (qui est une propriété ponctuelle) alors elle n'est pas nulle autour de ce point (propriété locale). Voici l'énoncé :

Lemme 4

Soit $f : I \to \mathbb{R}$ une fonction définie sur un intervalle I et x_0 un point de I. Si f est continue en x_0 et si $f(x_0) \neq 0$, alors il existe $\delta > 0$ tel que

$$\forall x \in]x_0 - \delta, x_0 + \delta[\quad f(x) \neq 0$$



Démonstration

Supposons par exemple que $f(x_0) > 0$, le cas $f(x_0) < 0$ se montrerait de la même manière. Écrivons ainsi la définition de la continuité de f en x_0 :

$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad x \in]x_0 - \delta, x_0 + \delta[\implies f(x_0) - \varepsilon < f(x) < f(x_0) + \varepsilon.$$

Il suffit donc de choisir ε tel que $0 < \varepsilon < f(x_0)$. Il existe alors bien un intervalle $J = I \cap]x_0 - \delta, x_0 + \delta[$ tel que pour tout x dans J, on a $f(x) > 0$.

La continuité se comporte bien avec les opérations élémentaires. Les propositions suivantes sont des conséquences immédiates des propositions analogues sur les limites.

Proposition 61

Soient $f, g : I \to \mathbb{R}$ deux fonctions continues en un point $x_0 \in I$. Alors

- $\lambda \cdot f$ est continue en x_0 (pour tout $\lambda \in \mathbb{R}$),
- $f + g$ est continue en x_0,
- $f \times g$ est continue en x_0,
- si $f(x_0) \neq 0$, alors $\frac{1}{f}$ est continue en x_0.

Exemple 96

La proposition précédente permet de vérifier que d'autres fonctions usuelles sont continues :

- les fonctions puissance $x \mapsto x^n$ sur $\mathbb{R}$ (comme produit $x \times x \times \cdots$),
- les polynômes sur $\mathbb{R}$ (somme et produit de fonctions puissance et de fonctions constantes),
- les fractions rationnelles $x \mapsto \frac{P(x)}{Q(x)}$ sur tout intervalle où le polynôme $Q(x)$ ne s'annule pas.

La composition conserve la continuité (mais il faut faire attention en quels points les hypothèses s'appliquent).

Proposition 62

Soient $f : I \to \mathbb{R}$ et $g : J \to \mathbb{R}$ deux fonctions telles que $f(I) \subset J$. Si f est continue en un point $x_0 \in I$ et si g est continue en $f(x_0)$, alors $g \circ f$ est continue en x_0.

3.3. Prolongement par continuité

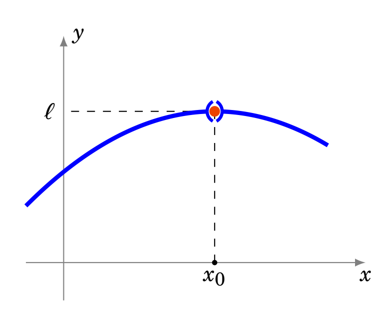
Définition 56

Soit I un intervalle, x_0 un point de I et $f : I \setminus \{x_0\} \to \mathbb{R}$ une fonction.

- On dit que f est ***prolongeable par continuité*** en x_0 si f admet une limite finie en x_0. Notons alors $\ell = \lim_{x_0} f$.
- On définit alors la fonction $\tilde{f} : I \to \mathbb{R}$ en posant pour tout $x \in I$

$$\tilde{f}(x) = \begin{cases} f(x) & \text{si } x \neq x_0 \\ \ell & \text{si } x = x_0. \end{cases}$$

Alors $\tilde{f}$ est continue en x_0 et on l'appelle le ***prolongement par continuité*** de f en x_0.



Dans la pratique, on continuera souvent à noter f à la place de $\tilde{f}$.

Exemple 97

Considérons la fonction f définie sur $\mathbb{R}^*$ par $f(x) = x \sin\left(\frac{1}{x}\right)$. Voyons si f admet un prolongement par continuité en 0 ?

Comme pour tout $x \in \mathbb{R}^*$ on a $|f(x)| \leqslant |x|$, on en déduit que f tend vers 0 en 0. Elle est donc prolongeable par continuité en 0 et son prolongement est la fonction $\tilde{f}$ définie sur $\mathbb{R}$ tout entier par :

$$\tilde{f}(x) = \begin{cases} x \sin\left(\frac{1}{x}\right) & \text{si } x \neq 0 \\ 0 & \text{si } x = 0. \end{cases}$$

3.4. Suites et continuité

Proposition 63

Soit $f : I \to \mathbb{R}$ une fonction et x_0 un point de I. Alors :

$$f \text{ est continue en } x_0 \iff \begin{array}{c}\text{pour toute suite } (u_n) \text{ qui converge vers } x_0 \\ \text{la suite } (f(u_n)) \text{ converge vers } f(x_0)\end{array}$$

Démonstration

$\Longrightarrow$ *On suppose que f est continue en x_0 et que (u_n) est une suite qui converge vers x_0 et on veut montrer que $(f(u_n))$ converge vers $f(x_0)$.*
Soit $\varepsilon > 0$. Comme f est continue en x_0, il existe un $\delta > 0$ tel que

$$\forall x \in I \quad |x - x_0| < \delta \implies |f(x) - f(x_0)| < \varepsilon.$$

Pour ce δ, comme (u_n) converge vers x_0, il existe $N \in \mathbb{N}$ tel que

$$\forall n \in \mathbb{N} \quad n \geqslant N \implies |u_n - x_0| < \delta.$$

On en déduit que, pour tout $n \geqslant N$, comme $|u_n - x_0| < \delta$, on a $|f(u_n) - f(x_0)| < \varepsilon$ et donc $(f(u_n))$ converge vers $f(x_0)$.

$\Longleftarrow$ *On va montrer la contraposée : supposons que f n'est pas continue en x_0 et montrons qu'alors il existe une suite (u_n) qui converge vers x_0 et telle que $(f(u_n))$ ne converge pas vers $f(x_0)$.*
Par hypothèse, comme f n'est pas continue en x_0 :

$$\exists \varepsilon_0 > 0 \quad \forall \delta > 0 \quad \exists x_\delta \in I \quad \text{tel que} \quad |x_\delta - x_0| < \delta \text{ et } |f(x_\delta) - f(x_0)| > \varepsilon_0.$$

On construit la suite (u_n) de la façon suivante : pour tout $n \in \mathbb{N}^*$, on choisit dans l'assertion précédente $\delta = 1/n$ et on obtient qu'il existe u_n (qui est $x_{1/n}$) tel que

$$|u_n - x_0| < \frac{1}{n} \quad \text{et} \quad |f(u_n) - f(x_0)| > \varepsilon_0.$$

La suite (u_n) converge vers x_0 alors que la suite $(f(u_n))$ ne peut pas converger vers $f(x_0)$.

Remarque

On retiendra surtout l'implication : si f est continue sur I et si (u_n) est une suite convergente de limite ℓ, alors $(f(u_n))$ converge vers $f(\ell)$. On l'utilisera intensivement pour l'étude des suites récurrentes $u_{n+1} = f(u_n)$: si f est continue et $u_n \to \ell$, alors $f(\ell) = \ell$.

Mini-exercices

1. Déterminer le domaine de définition et de continuité des fonctions suivantes : $f(x) = 1/\sin x$, $g(x) = 1/\sqrt{x + \frac{1}{2}}$, $h(x) = \ln(x^2 + x - 1)$.
2. Trouver les couples $(a, b) \in \mathbb{R}^2$ tels que la fonction f définie sur $\mathbb{R}$ par $f(x) = ax + b$ si $x < 0$ et $f(x) = \exp(x)$ si $x \geqslant 0$ soit continue sur $\mathbb{R}$. Et si on avait $f(x) = \frac{a}{x-1} + b$ pour $x < 0$?
3. Soit f une fonction continue telle que $f(x_0) = 1$. Montrer qu'il existe $\delta > 0$ tel que : pour tout $x \in]x_0 - \delta, x_0 + \delta[\quad f(x) > \frac{1}{2}$.

4. Étudier la continuité de $f : \mathbb{R} \to \mathbb{R}$ définie par : $f(x) = \sin(x)\cos\left(\frac{1}{x}\right)$ si $x \neq 0$ et $f(0) = 0$. Et pour $g(x) = xE(x)$?
5. La fonction définie par $f(x) = \frac{x^3+8}{|x+2|}$ admet-elle un prolongement par continuité en -2 ?
6. Soit la suite définie par $u_0 > 0$ et $u_{n+1} = \sqrt{u_n}$. Montrer que (u_n) admet une limite $\ell \in \mathbb{R}$ lorsque $n \to +\infty$. À l'aide de la fonction $f(x) = \sqrt{x}$ calculer cette limite.

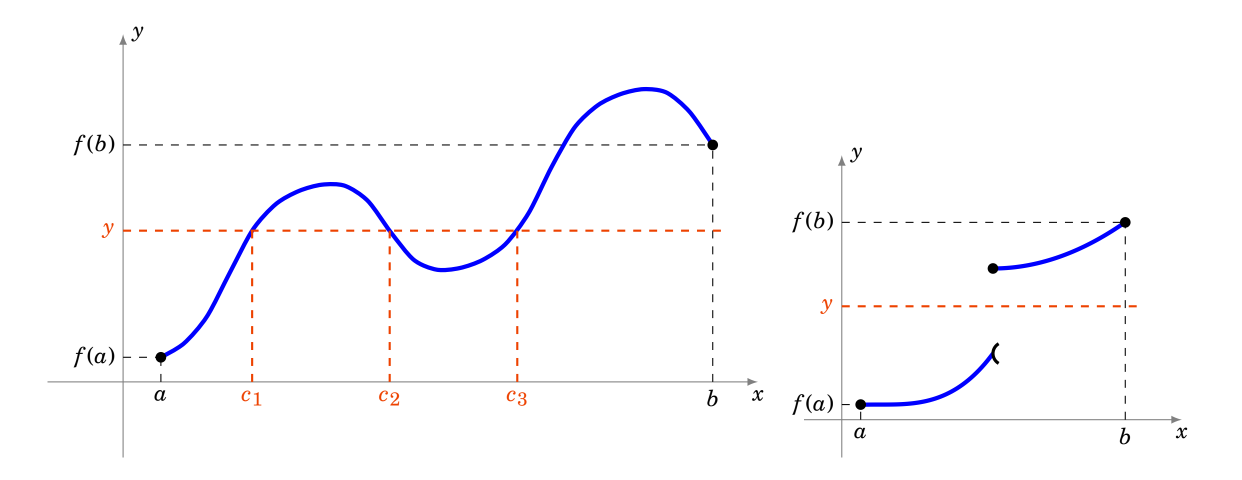
4. Continuité sur un intervalle

4.1. Le théorème des valeurs intermédiaires

Théorème 22. Théorème des valeurs intermédiaires

Soit $f : [a, b] \to \mathbb{R}$ une fonction continue sur un segment.

Pour tout réel y compris entre $f(a)$ et $f(b)$, il existe $c \in [a, b]$ tel que $f(c) = y$.



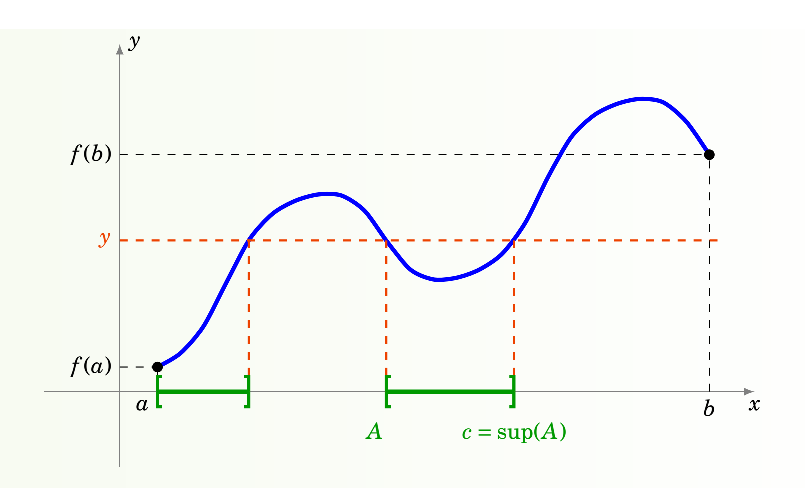
Démonstration

Montrons le théorème dans le cas où $f(a) < f(b)$. On considère alors un réel y tel que $f(a) \leqslant y \leqslant f(b)$ et on veut montrer qu'il a un antécédent par f.

1. On introduit l'ensemble suivant

$$A = \left\{x \in [a, b] \mid f(x) \leqslant y\right\}.$$

Tout d'abord l'ensemble A est non vide (car $a \in A$) et il est majoré (car il est contenu dans $[a, b]$) : il admet donc une borne supérieure, que l'on note $c = \sup A$. Montrons que $f(c) = y$.



2. Montrons tout d'abord que $f(c) \leqslant y$. Comme $c = \sup A$, il existe une suite $(u_n)_{n\in\mathbb{N}}$ contenue dans A telle que (u_n) converge vers c. D'une part, pour tout $n \in \mathbb{N}$, comme $u_n \in A$, on a $f(u_n) \leqslant y$. D'autre part, comme f est continue en c, la suite $(f(u_n))$ converge vers $f(c)$. On en déduit donc, par passage à la limite, que $f(c) \leqslant y$.
3. Montrons à présent que $f(c) \geqslant y$. Remarquons tout d'abord que si $c = b$, alors on a fini, puisque $f(b) \geqslant y$. Sinon, pour tout $x \in]c, b]$, comme $x \notin A$, on a $f(x) > y$. Or, étant donné que f est continue en c, f admet une limite à droite en c, qui vaut $f(c)$ et on obtient $f(c) \geqslant y$.

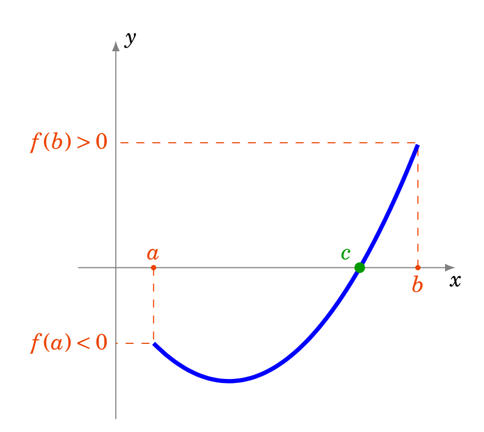
4.2. Applications du théorème des valeurs intermédiaires

Voici la version la plus utilisée du théorème des valeurs intermédiaires.

Corollaire 11

Soit $f : [a, b] \to \mathbb{R}$ une fonction continue sur un segment.

Si $f(a) \cdot f(b) < 0$, alors il existe $c \in]a, b[$ tel que $f(c) = 0$.

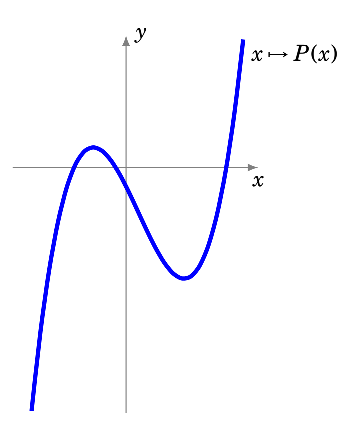


Démonstration

Il s'agit d'une application directe du théorème des valeurs intermédiaires avec $y = 0$. L'hypothèse $f(a) \cdot f(b) < 0$ signifiant que $f(a)$ et $f(b)$ sont de signes contraires.

Exemple 98

Tout polynôme de degré impair possède au moins une racine réelle.

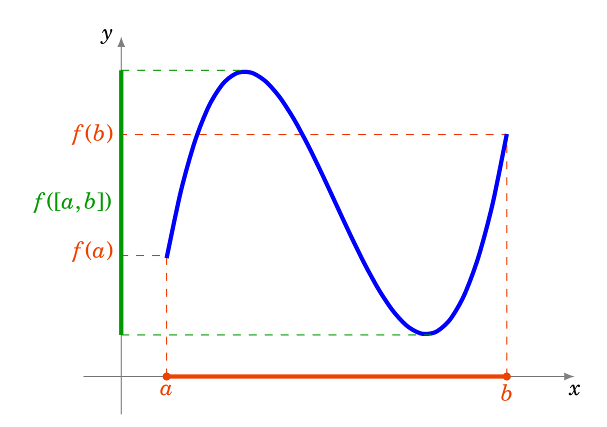


En effet, un tel polynôme s'écrit $P(x) = a_n x^n + \cdots + a_1 x + a_0$ avec n un entier impair. On peut supposer que le coefficient a_n est strictement positif. Alors on a $\lim_{-\infty} P = -\infty$ et $\lim_{+\infty} P = +\infty$. En particulier, il existe deux réels a et b tels que $f(a) < 0$ et $f(b) > 0$ et on conclut grâce au corollaire précédent.

Corollaire 12

Soit $f : I \to \mathbb{R}$ une fonction continue sur un intervalle I. Alors $f(I)$ est un intervalle.

Attention ! Il serait faux de croire que l'image par une fonction f de l'intervalle $[a,b]$ soit l'intervalle $[f(a), f(b)]$.



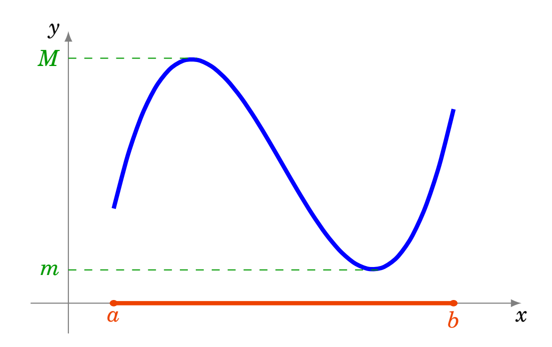
Démonstration

Soient $y_1, y_2 \in f(I)$, $y_1 \leqslant y_2$. Montrons que si $y \in [y_1, y_2]$, alors $y \in f(I)$. Par hypothèse, il existe $x_1, x_2 \in I$ tels que $y_1 = f(x_1)$, $y_2 = f(x_2)$ et donc y est compris entre $f(x_1)$ et $f(x_2)$. D'après le théorème des valeurs intermédiaires, comme f est continue, il existe donc $x \in I$ tel que $y = f(x)$, et ainsi $y \in f(I)$.

4.3. Fonctions continues sur un segment

Théorème 23

Soit $f : [a,b] \to \mathbb{R}$ une fonction continue sur un segment. Alors il existe deux réels m et M tels que $f([a,b]) = [m,M]$. Autrement dit, l'image d'un segment par une fonction continue est un segment.



Comme on sait déjà par le théorème des valeurs intermédiaires que $f([a,b])$ est un intervalle, le théorème précédent signifie exactement que

Si f est continue sur $[a,b]$ alors f est bornée sur $[a,b]$ et elle atteint ses bornes.

Donc m est le minimum de la fonction sur l'intervalle $[a,b]$ alors que M est le maximum.
[[Preuve : à écrire]]

Mini-exercices

1. Soient $P(x) = x^5 - 3x - 2$ et $f(x) = x2^x - 1$ deux fonctions définies sur $\mathbb{R}$. Montrer que l'équation $P(x) = 0$ a au moins une racine dans $[1,2]$; l'équation $f(x) = 0$ a au moins une racine dans $[0,1]$; l'équation $P(x) = f(x)$ a au moins une racine dans $]0,2[$.
2. Montrer qu'il existe $x > 0$ tel que $2^x + 3^x = 5^x$.
3. Dessiner le graphe d'une fonction continue $f : \mathbb{R} \to \mathbb{R}$ tel que $f(\mathbb{R}) = [0,1]$. Puis $f(\mathbb{R}) =]0,1[$; $f(\mathbb{R}) = [0,1[$; $f(\mathbb{R}) =]-\infty,1]$, $f(\mathbb{R}) =]-\infty,1[$.
4. Soient $f,g : [0,1] \to \mathbb{R}$ deux fonctions continues. Quelles fonctions suivantes sont à coup sûr bornées : $f+g$, $f \times g$, f/g ?
5. Soient f et g deux fonctions continues sur $[0,1]$ telles que $\forall x \in [0,1]\ f(x) < g(x)$. Montrer qu'il existe $m > 0$ tel que $\forall x \in [0,1]\ f(x)+m < g(x)$. Ce résultat est-il vrai si on remplace $[0,1]$ par $\mathbb{R}$?

5. Fonctions monotones et bijections

5.1. Rappels : injection, surjection, bijection

Dans cette section nous rappelons le matériel nécessaire concernant les applications bijectives.

Définition 57

Soit $f : E \to F$ une fonction, où E et F sont des parties de $\mathbb{R}$.

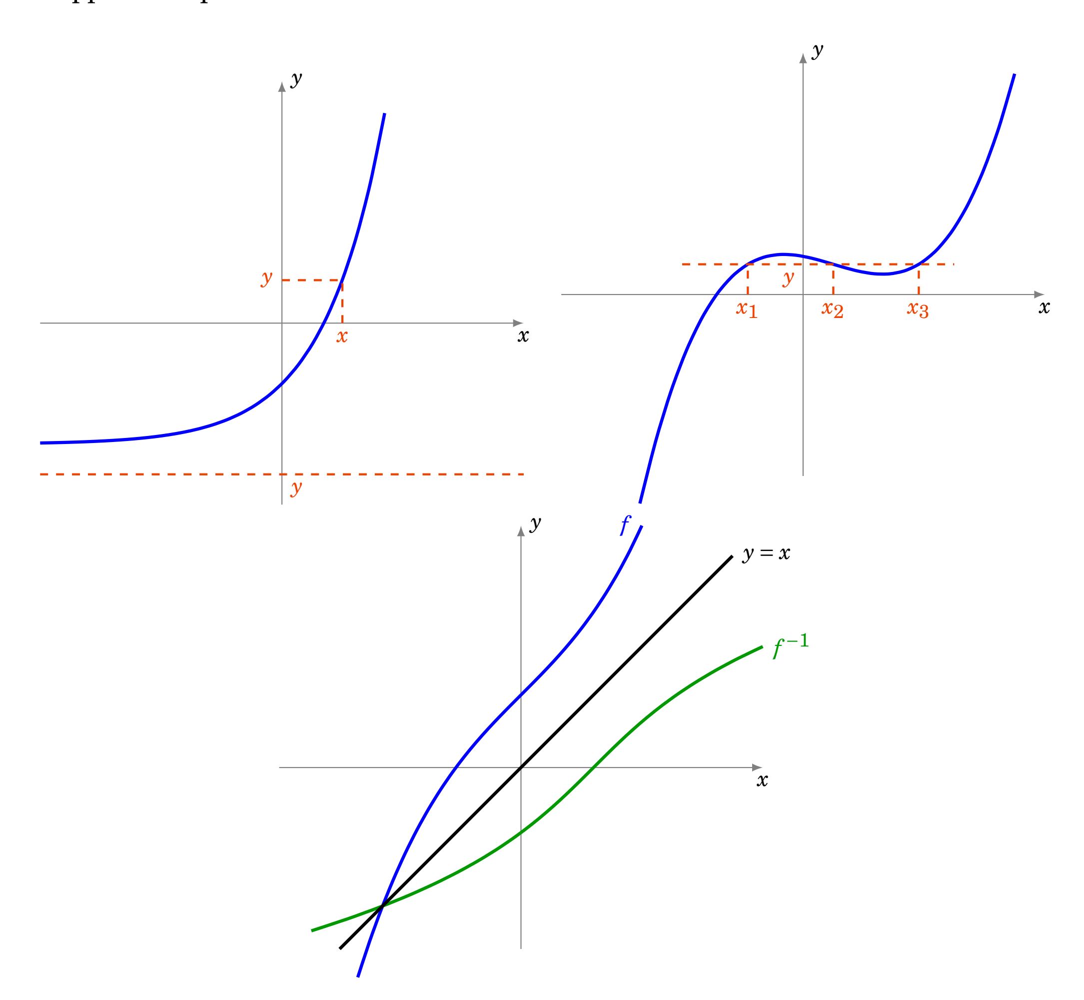
- f est ***injective*** si $\forall x, x' \in E \quad f(x) = f(x') \implies x = x'$;
- f est ***surjective*** si $\forall y \in F \quad \exists x \in E \quad y = f(x)$;
- f est ***bijective*** si f est à la fois injective et surjective, c'est-à-dire si $\forall y \in F \quad \exists! x \in E \quad y = f(x)$.

Proposition 64

Si $f : E \to F$ est une fonction bijective alors il existe une unique application $g : F \to E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$ La fonction g est la ***bijection réciproque*** de f et se note f^{-1}.

Remarque

- On rappelle que l'***identité***, $\mathrm{id}_E : E \to E$ est simplement définie par $x \mapsto x$.
- $g \circ f = \mathrm{id}_E$ se reformule ainsi : $\forall x \in E \quad g\big(f(x)\big) = x$.
- Alors que $f \circ g = \mathrm{id}_F$ s'écrit : $\forall y \in F \quad f\big(g(y)\big) = y$.
- Dans un repère orthonormé les graphes des fonctions f et f^{-1} sont symétriques par rapport à la première bissectrice.



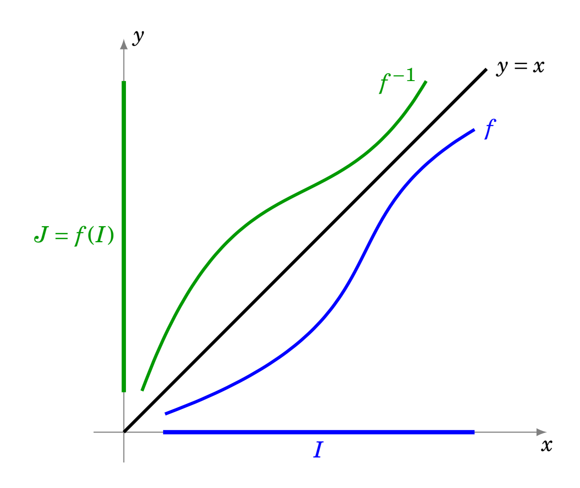
5.2. Fonctions monotones et bijections

Voici un résultat important qui permet d'obtenir des fonctions bijectives.

Théorème 24. Théorème de la bijection

Soit $f : I \to \mathbb{R}$ une fonction définie sur un intervalle I de $\mathbb{R}$. Si f est continue et strictement monotone sur I, alors

1. f établit une bijection de l'intervalle I dans l'intervalle image $J = f(I)$,
2. la fonction réciproque $f^{-1} : J \to I$ est continue et strictement monotone sur J et elle a le même sens de variation que f.



En pratique, si on veut appliquer ce théorème à une fonction continue $f : I \to \mathbb{R}$, on découpe l'intervalle I en sous-intervalles sur lesquels la fonction f est strictement monotone.

Exemple 99

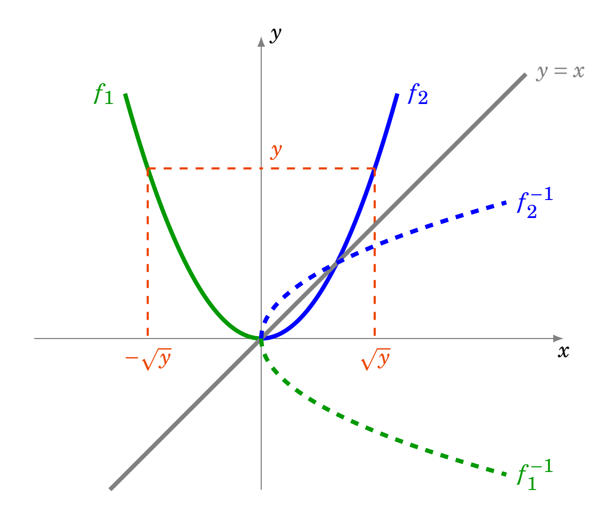
Considérons la fonction carrée définie sur $\mathbb{R}$ par $f(x) = x^2$. La fonction f n'est pas strictement monotone sur $\mathbb{R}$, d'ailleurs, on voit bien qu'elle n'est pas injective. Cependant, en restreignant son ensemble de définition à $]-\infty, 0]$ d'une part et à $[0, +\infty[$ d'autre part, on définit deux fonctions strictement monotones (les ensembles de départ sont différents) :

$$f_1 : \begin{cases}]-\infty, 0] \longrightarrow [0, +\infty[\\ x \longmapsto x^2 \end{cases} \quad \text{et} \quad f_2 : \begin{cases} [0, +\infty[\longrightarrow [0, +\infty[\\ x \longmapsto x^2 \end{cases}$$

On remarque que $f(]-\infty, 0]) = f([0, +\infty[) = [0, +\infty[$. D'après le théorème précédent, les fonctions f_1 et f_2 sont des bijections. Déterminons leurs fonctions réciproques $f_1^{-1} : [0, +\infty[\to]-\infty, 0]$ et $f_2^{-1} : [0, +\infty[\to [0, +\infty[$. Soient deux réels x et y tels que $y \geqslant 0$. Alors

$$\begin{aligned} y = f(x) &\Leftrightarrow y = x^2 \\ &\Leftrightarrow x = \sqrt{y} \quad \text{ou} \quad x = -\sqrt{y}, \end{aligned}$$

c'est-à-dire y admet deux antécédents, l'un dans $[0, +\infty[$ et l'autre dans $]-\infty, 0]$. Et donc $f_1^{-1}(y) = -\sqrt{y}$ et $f_2^{-1}(y) = \sqrt{y}$. On retrouve bien que chacune des deux fonctions f_1 et f_2 a le même sens de variation que sa réciproque.



On remarque que la courbe totale en pointillée (à la fois la partie bleue et la verte), qui est l'image du graphe de f par la symétrie par rapport à la première bissectrice, ne peut pas être le graphe d'une fonction : c'est une autre manière de voir que f n'est pas bijective.

Généralisons l'exemple précédent.

Exemple 100

Soit $n \geqslant 1$. Soit $f : [0,+\infty[\to [0,+\infty[$ définie par $f(x) = x^n$. Alors f est continue et strictement croissante. Comme $\lim_{+\infty} f = +\infty$ alors f est une bijection. Sa bijection réciproque f^{-1} est notée : $x \mapsto x^{\frac{1}{n}}$ (ou aussi $x \mapsto \sqrt[n]{x}$) : c'est la fonction racine n-ième. Elle est continue et strictement croissante.

5.3. Démonstration

On établit d'abord un lemme utile à la démonstration du théorème précédent.

Lemme 5

Soit $f : I \to \mathbb{R}$ une fonction définie sur un intervalle I de $\mathbb{R}$. Si f est strictement monotone sur I, alors f est injective sur I.

Démonstration

Soient $x, x' \in I$ tels que $f(x) = f(x')$. Montrons que $x = x'$. Si on avait $x < x'$, alors on aurait nécessairement $f(x) < f(x')$ ou $f(x) > f(x')$, suivant que f est strictement croissante, ou strictement décroissante. Comme c'est impossible, on en déduit que $x \geqslant x'$. En échangeant les rôles de x et de x', on montre de même que $x \leqslant x'$. On en conclut que $x = x'$ et donc que f est injective.

Démonstration . Démonstration du théorème

1. D'après le lemme précédent, f est injective sur I. En restreignant son ensemble d'arrivée à son image $J = f(I)$, on obtient que f établit une bijection de I dans J. Comme f est continue, par le théorème des valeurs intermédiaires, l'ensemble J est un intervalle.
2. Supposons pour fixer les idées que f est strictement croissante.
   (a) Montrons que f^{-1} est strictement croissante sur J. Soient $y, y' \in J$ tels que $y < y'$. Notons

$x = f^{-1}(y) \in I$ et $x' = f^{-1}(y') \in I$. Alors $y = f(x)$, $y' = f(x')$ et donc

$$\begin{aligned} y < y' &\implies f(x) < f(x') \\ &\implies x < x' \qquad \text{(car } f \text{ est strictement croissante)} \\ &\implies f^{-1}(y) < f^{-1}(y'), \end{aligned}$$

c'est-à-dire f^{-1} est strictement croissante sur J.

(b) Montrons que f^{-1} est continue sur J. On se limite au cas où I est de la forme $]a,b[$, les autres cas se montrent de la même manière. Soit $y_0 \in J$. On note $x_0 = f^{-1}(y_0) \in I$. Soit $\varepsilon > 0$. On peut toujours supposer que $[x_0-\varepsilon, x_0+\varepsilon] \subset I$. On cherche un réel $\delta > 0$ tel que pour tout $y \in J$ on ait

$$y_0 - \delta < y < y_0 + \delta \implies f^{-1}(y_0) - \varepsilon < f^{-1}(y) < f^{-1}(y_0) + \varepsilon$$

c'est-à-dire tel que pour tout $x \in I$ on ait

$$y_0 - \delta < f(x) < y_0 + \delta \implies f^{-1}(y_0) - \varepsilon < x < f^{-1}(y_0) + \varepsilon.$$

Or, comme f est strictement croissante, on a pour tout $x \in I$

$$\begin{aligned} f(x_0-\varepsilon) < f(x) < f(x_0+\varepsilon) &\implies x_0 - \varepsilon < x < x_0 + \varepsilon \\ &\implies f^{-1}(y_0) - \varepsilon < x < f^{-1}(y_0) + \varepsilon. \end{aligned}$$

Comme $f(x_0-\varepsilon) < y_0 < f(x_0+\varepsilon)$, on peut choisir le réel $\delta > 0$ tel que

$$f(x_0-\varepsilon) < y_0 - \delta \quad \text{et} \quad f(x_0+\varepsilon) > y_0 + \delta$$

et on a bien alors pour tout $x \in I$

$$\begin{aligned} y_0 - \delta < f(x) < y_0 + \delta &\implies f(x_0-\varepsilon) < f(x) < f(x_0+\varepsilon) \\ &\implies f^{-1}(y_0) - \varepsilon < x < f^{-1}(y_0) + \varepsilon. \end{aligned}$$

La fonction f^{-1} est donc continue sur J.

Mini-exercices

1. Montrer que chacune des hypothèses « continue » et « strictement monotone » est nécessaire dans l'énoncé du théorème.
2. Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^3 + x$. Montrer que f est bijective, tracer le graphe de f et de f^{-1}.
3. Soit $n \geqslant 1$. Montrer que $f(x) = 1 + x + x^2 + \cdots + x^n$ définit une bijection de l'intervalle $[0,1]$ vers un intervalle à préciser.
4. Existe-t-il une fonction continue : $f : [0,1[\to]0,1[$ qui soit bijective ? $f : [0,1[\to]0,1[$ qui soit injective ? $f :]0,1[\to [0,1]$ qui soit surjective ?
5. Pour $y \in \mathbb{R}$ on considère l'équation $x + \exp x = y$. Montrer qu'il existe une unique solution y. Comment varie y en fonction de x ? Comme varie x en fonction de y ?

Auteurs

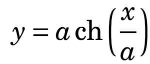
Auteurs : Arnaud Bodin, Niels Borne, Laura Desideri
Dessins : Benjamin Boutin

Exo7

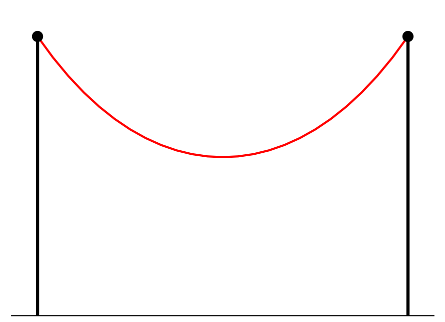
9 Fonctions usuelles

Vidéo ■ partie 1. Logarithme et exponentielle
Vidéo ■ partie 2. Fonctions circulaires inverses
Vidéo ■ partie 3. Fonctions hyperboliques et hyperboliques inverses

Vous connaissez déjà des fonctions classiques : $\exp, \ln, \cos, \sin, \tan$. Dans ce chapitre il s'agit d'ajouter à notre catalogue de nouvelles fonctions : $\text{ch}, \text{sh}, \text{th}, \arccos, \arcsin, \arctan, \text{Argch}, \text{Argsh}, \text{Argth}$. Ces fonctions apparaissent naturellement dans la résolution de problèmes simples, en particulier issus de la physique. Par exemple lorsqu'un fil est suspendu entre deux poteaux (ou un collier tenu entre deux mains) alors la courbe dessinée est une ***chaînette*** dont l'équation fait intervenir le cosinus hyperbolique et un paramètre a (qui dépend de la longueur du fil et de l'écartement des poteaux) :



$$y = a\,\text{ch}\left(\frac{x}{a}\right)$$



1. Logarithme et exponentielle

1.1. Logarithme

Proposition 65

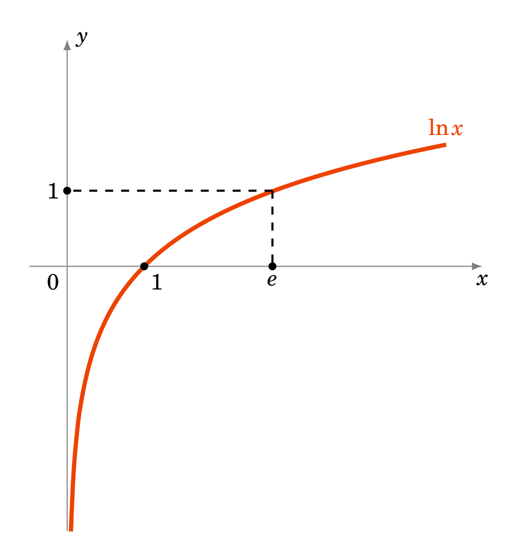
Il existe une unique fonction, notée $\ln :]0,+\infty[\to \mathbb{R}$ telle que :

$$\ln'(x) = \frac{1}{x} \quad \text{(pour tout } x > 0) \qquad \text{et} \qquad \ln(1) = 0.$$

De plus cette fonction vérifie (pour tout $a, b > 0$) :

1. $\ln(a \times b) = \ln a + \ln b$,
2. $\ln(\frac{1}{a}) = -\ln a$,
3. $\ln(a^n) = n \ln a$, (pour tout $n \in \mathbb{N}$)
4. $\ln$ est une fonction continue, strictement croissante et définit une bijection de $]0,+\infty[$ sur $\mathbb{R}$,

5. $\lim_{x\to 0} \frac{\ln(1+x)}{x} = 1$,
6. la fonction ln est concave et $\ln x \leqslant x - 1$ (pour tout $x > 0$).



Remarque

$\ln x$ s'appelle le ***logarithme naturel*** ou aussi ***logarithme néperien***. Il est caractérisé par $\ln(e) = 1$. On définit le ***logarithme en base a*** par

$$\log_a(x) = \frac{\ln(x)}{\ln(a)}$$

De sorte que $\log_a(a) = 1$.

Pour $a = 10$ on obtient le ***logarithme décimal*** $\log_{10}$ qui vérifie $\log_{10}(10) = 1$ (et donc $\log_{10}(10^n) = n$). Dans la pratique on utilise l'équivalence : $\boxed{x = 10^y \iff y = \log_{10}(x)}$ En informatique intervient aussi le logarithme en base 2 : $\log_2(2^n) = n$.

Démonstration

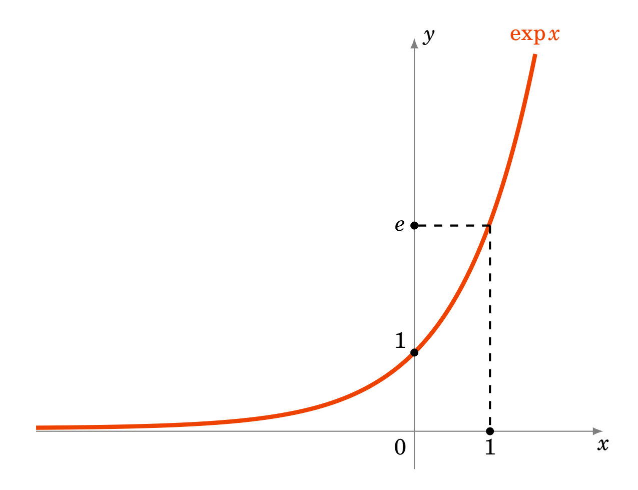
L'existence et l'unicité viennent de la théorie de l'intégrale : $\ln(x) = \int_1^x \frac{1}{t}\,dt$. Passons aux propriétés.

1. Posons $f(x) = \ln(xy) - \ln(x)$ où $y > 0$ est fixé. Alors $f'(x) = y\ln'(xy) - \ln'(x) = \frac{y}{xy} - \frac{1}{x} = 0$. Donc $x \mapsto f(x)$ a une dérivée nulle, donc est constante et vaut $f(1) = \ln(y) - \ln(1) = \ln(y)$. Donc $\ln(xy) - \ln(x) = \ln(y)$.
2. D'une part $\ln(a \times \frac{1}{a}) = \ln a + \ln \frac{1}{a}$, mais d'autre part $\ln(a \times \frac{1}{a}) = ln(1) = 0$. Donc $\ln a + \ln \frac{1}{a} = 0$.
3. Similaire ou récurrence.
4. ln est dérivable donc continue, $\ln'(x) = \frac{1}{x} > 0$ donc la fonction est strictement croissante. Comme $\ln(2) > \ln(1) = 0$ alors $\ln(2^n) = n\ln(2) \to +\infty$ (lorsque $n \to +\infty$). Donc $\lim_{x\to+\infty} \ln x = +\infty$. De $\ln x = -\ln \frac{1}{x}$ on déduit $\lim_{x\to 0} \ln x = -\infty$. Par le théorème sur les fonctions continues et strictement croissantes, $\ln :]0, +\infty[\to \mathbb{R}$ est une bijection.
5. $\lim_{x\to 0} \frac{\ln(1+x)}{x}$ est la dérivée de ln au point $x_0 = 1$, donc cette limite existe et vaut $\ln'(1) = 1$.
6. $\ln'(x) = \frac{1}{x}$ est décroissante, donc la fonction ln est concave. Posons $f(x) = x - 1 - \ln x$; $f'(x) = 1 - \frac{1}{x}$. Par une étude de fonction f atteint son maximum en $x_0 = 1$. Donc $f(x) \geqslant f(1) = 0$. Donc $\ln x \leqslant x - 1$.

1.2. Exponentielle

Définition 58

La bijection réciproque de $\ln :]0,+\infty[\to \mathbb{R}$ s'appelle la fonction ***exponentielle***, notée $\exp : \mathbb{R} \to]0,+\infty[$.



Pour $x \in \mathbb{R}$ on note aussi e^x pour $\exp x$.

Proposition 66

La fonction exponentielle vérifie les propriétés suivantes :

- $\boxed{\exp(\ln x) = x \text{ pour tout } x > 0}$ et $\boxed{\ln(\exp x) = x \text{ pour tout } x \in \mathbb{R}}$
- $\exp(a+b) = \exp(a) \times \exp(b)$
- $\exp(nx) = (\exp x)^n$
- $\exp : \mathbb{R} \to]0,+\infty[$ est une fonction continue, strictement croissante vérifiant $\lim_{x\to-\infty} \exp x = 0$ et $\lim_{x\to+\infty} \exp = +\infty$.
- La fonction exponentielle est dérivable et $\exp' x = \exp x$, pour tout $x \in \mathbb{R}$. Elle est convexe et $\exp x \geqslant 1 + x$

Remarque

La fonction exponentielle est l'unique fonction qui vérifie $\exp'(x) = \exp(x)$ (pour tout $x \in \mathbb{R}$) et $\exp(1) = e$. Où $e \simeq 2,718\ldots$ est le nombre qui vérifie $\ln e = 1$.

Démonstration

Ce sont les propriétés du logarithme retranscrites pour sa bijection réciproque.
Par exemple pour la dérivée : on part de l'égalité $\ln(\exp x) = x$ que l'on dérive. Cela donne $\exp'(x) \times \ln'(\exp x) = 1$ donc $\exp'(x) \times \frac{1}{\exp x} = 1$ et ainsi $\exp'(x) = \exp x$.

1.3. Puissance et comparaison

Par définition, pour $a > 0$ et $b \in \mathbb{R}$,

$$\boxed{a^b = \exp\left(b \ln a\right)}$$

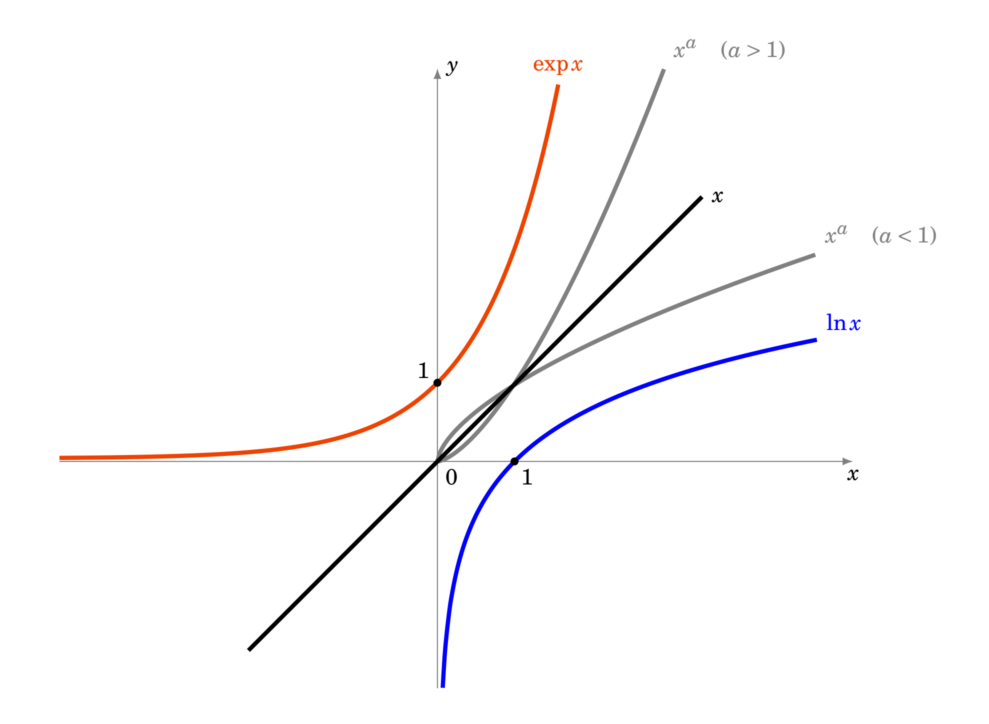
Remarque

- $\sqrt{a} = a^{\frac{1}{2}} = \exp\left(\frac{1}{2}\ln a\right)$
- $\sqrt[n]{a} = a^{\frac{1}{n}} = \exp\left(\frac{1}{n}\ln a\right)$ (la ***racine n-ième*** de a)
- On note aussi $\exp x$ par e^x ce qui se justifie par le calcul : $e^x = \exp\left(x\ln e\right) = \exp(x)$.
- Les fonctions $x \mapsto a^x$ s'appellent aussi des fonctions exponentielles et se ramènent systématiquement à la fonction exponentielle classique par l'égalité $a^x = \exp(x\ln a)$. Il ne faut surtout pas les confondre avec les fonctions puissances $x \mapsto x^a$.

Comparons les fonctions $\ln x$, $\exp x$ avec x :

Proposition 67

$$\lim_{x\to+\infty} \frac{\ln x}{x} = 0 \qquad \text{et} \qquad \lim_{x\to+\infty} \frac{\exp x}{x} = +\infty.$$



Démonstration

1. On a vu $\ln x \leqslant x - 1$ (pour tout $x > 0$). Donc $\ln x \leqslant x$ donc $\frac{\ln\sqrt{x}}{\sqrt{x}} \leqslant 1$. Cela donne
$$0 \leqslant \frac{\ln x}{x} = \frac{\ln\left(\sqrt{x}^2\right)}{x} = 2\frac{\ln\sqrt{x}}{x} = 2\frac{\ln\sqrt{x}}{\sqrt{x}}\frac{1}{\sqrt{x}} \leqslant \frac{2}{\sqrt{x}}$$
Cette double inégalité entraîne $\lim_{x\to+\infty}\frac{\ln x}{x} = 0$.
2. On a vu $\exp x \geqslant 1 + x$ (pour tout $x \in \mathbb{R}$). Donc $\exp x \to +\infty$ (lorsque $x \to +\infty$).
$$\frac{x}{\exp x} = \frac{\ln(\exp x)}{\exp x} = \frac{\ln u}{u}$$
lorsque $x \to +\infty$ alors $u = \exp x \to +\infty$ et donc par le premier point $\frac{\ln u}{u} \to 0$. Donc $\frac{x}{\exp x} \to 0$ et reste positive, ainsi $\lim_{x\to+\infty}\frac{\exp x}{x} = +\infty$.

Mini-exercices

1. Montrer que $\ln(1+e^x) = x + \ln(1+e^{-x})$, pour tout $x \in \mathbb{R}$.
2. Étudier la fonction $f(x) = \ln(x^2+1) - \ln(x) - 1$. Tracer son graphe. Résoudre l'équation $(f(x) = 0)$. Idem avec $g(x) = \frac{1+\ln x}{x}$. Idem avec $h(x) = x^x$.
3. Expliquer comment $\log_{10}$ permet de calculer le nombre de chiffres d'un entier n.
4. Montrer $\ln(1+x) \geqslant x - \frac{x^2}{2}$ pour $x \geqslant 0$ (faire une étude de fonction). Idem avec $e^x \geqslant 1+x+\frac{x^2}{2}$ pour tout $x \geqslant 0$.
5. Calculer la limite de la suite définie par $u_n = \left(1+\frac{1}{n}\right)^n$ lorsque $n \to +\infty$. Idem avec $v_n = \left(\frac{1}{n}\right)^n$ et $w_n = n^{\frac{1}{n}}$.

2. Fonctions circulaires inverses

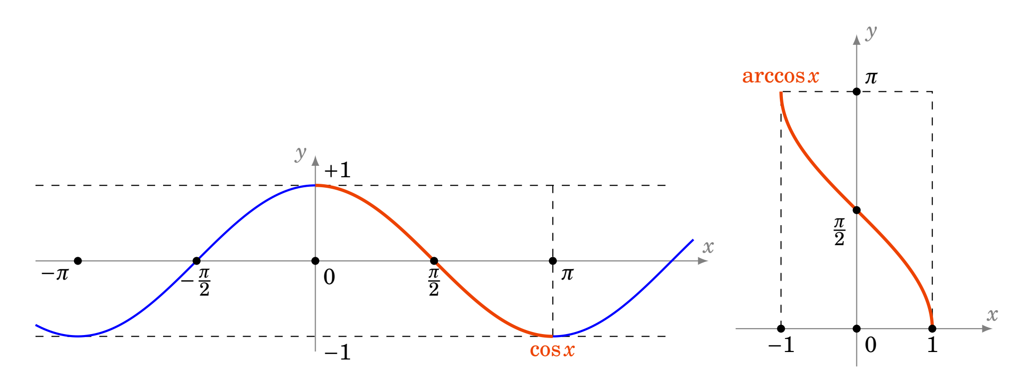
2.1. Arccosinus

Considérons la fonction cosinus $\cos : \mathbb{R} \to [-1,1]$, $x \mapsto \cos x$. Pour obtenir une bijection à partir de cette fonction, il faut considérer la restriction de cosinus à l'intervalle $[0,\pi]$. Sur cet intervalle la fonction cosinus est continue et strictement décroissante, donc la restriction

$$\cos_| : [0,\pi] \to [-1,1]$$

est une bijection. Sa bijection réciproque est la fonction ***arccosinus*** :

$$\arccos : [-1,1] \to [0,\pi]$$



On a donc, par définition de la bijection réciproque :

$$\cos\big(\arccos(x)\big) = x \quad \forall x \in [-1,1]$$
$$\arccos\big(\cos(x)\big) = x \quad \forall x \in [0,\pi]$$

Autrement dit :

$$\text{Si} \quad x \in [0,\pi] \qquad \cos(x) = y \iff x = \arccos y$$

Terminons avec la dérivée de arccos :

$$\arccos'(x) = \frac{-1}{\sqrt{1-x^2}} \qquad \forall x \in]-1,1[$$

Démonstration

On démarre de l'égalité $\cos(\arccos x) = x$ que l'on dérive :

$$\begin{aligned}
&\cos(\arccos x) = x \\
\implies &-\arccos'(x) \times \sin(\arccos x) = 1 \\
\implies &\arccos'(x) = \frac{-1}{\sin(\arccos x)} \\
\implies &\arccos'(x) = \frac{-1}{\sqrt{1-\cos^2(\arccos x)}} \qquad (*) \\
\implies &\arccos'(x) = \frac{-1}{\sqrt{1-x^2}}
\end{aligned}$$

Le point crucial $(*)$ se justifie ainsi : on démarre de l'égalité $\cos^2 y + \sin^2 y = 1$, en substituant $y = \arccos x$ on obtient $\cos^2(\arccos x) + \sin^2(\arccos x) = 1$ donc $x^2 + \sin^2(\arccos x) = 1$. On en déduit : $\sin(\arccos x) = +\sqrt{1-x^2}$ (avec le signe + car $\arccos x \in [0, \pi]$).

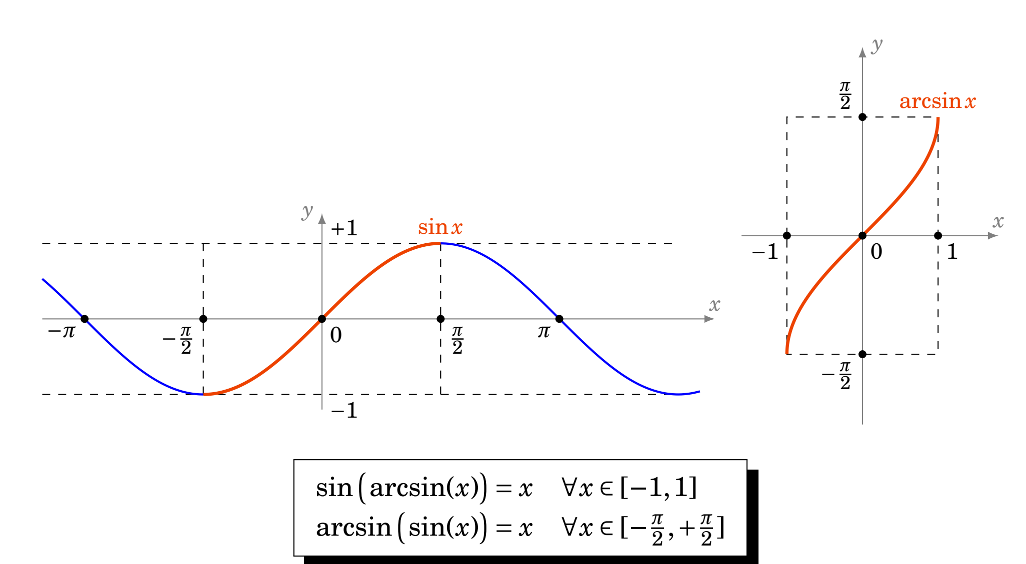
2.2. Arcsinus

La restriction

$$\sin_| : [-\frac{\pi}{2}, +\frac{\pi}{2}] \to [-1, 1]$$

est une bijection. Sa bijection réciproque est la fonction ***arcsinus*** :

$$\arcsin : [-1, 1] \to [-\frac{\pi}{2}, +\frac{\pi}{2}]$$



$$\sin\big(\arcsin(x)\big) = x \quad \forall x \in [-1, 1]$$
$$\arcsin\big(\sin(x)\big) = x \quad \forall x \in [-\tfrac{\pi}{2}, +\tfrac{\pi}{2}]$$

Si $x \in [-\frac{\pi}{2}, +\frac{\pi}{2}]$ $\quad \sin(x) = y \iff x = \arcsin y$

$$\arcsin'(x) = \frac{1}{\sqrt{1-x^2}} \qquad \forall x \in]-1, 1[$$

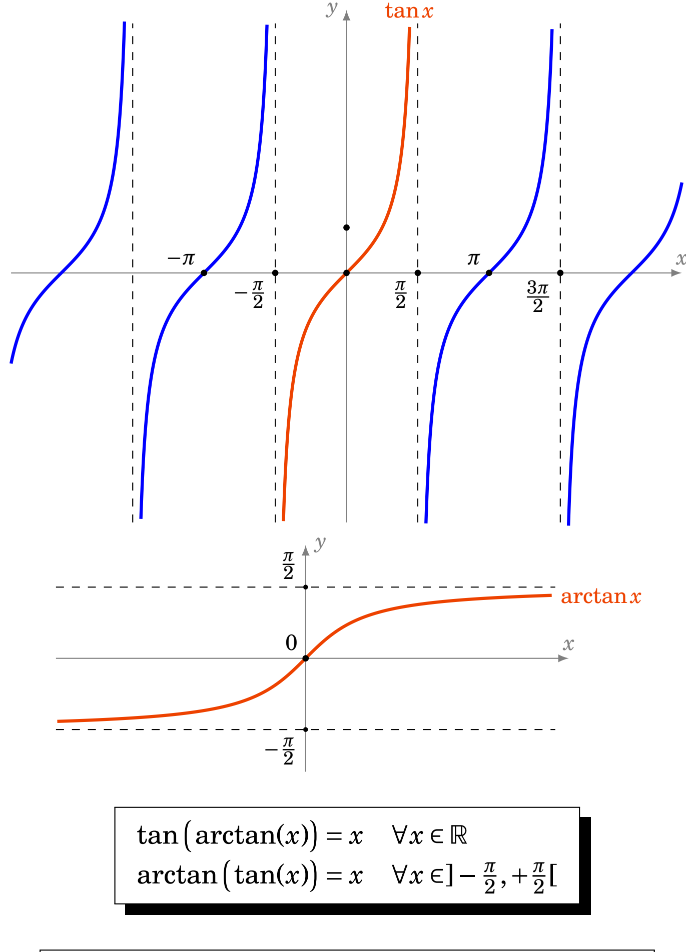
2.3. Arctangente

La restriction

$$\tan_| :]-\frac{\pi}{2}, +\frac{\pi}{2}[\to \mathbb{R}$$

est une bijection. Sa bijection réciproque est la fonction ***arctangente*** :

$$\arctan : \mathbb{R} \to]-\frac{\pi}{2}, +\frac{\pi}{2}[$$



$$\tan\big(\arctan(x)\big) = x \quad \forall x \in \mathbb{R}$$
$$\arctan\big(\tan(x)\big) = x \quad \forall x \in]-\tfrac{\pi}{2}, +\tfrac{\pi}{2}[$$

$$\text{Si} \quad x \in]-\tfrac{\pi}{2}, +\tfrac{\pi}{2}[\qquad \tan(x) = y \iff x = \arctan y$$

$$\arctan'(x) = \frac{1}{1+x^2} \qquad \forall x \in \mathbb{R}$$

Mini-exercices

1. Calculer les valeurs de arccos et arcsin en 0, 1, $\frac{1}{2}$, $\frac{\sqrt{2}}{2}$, $\frac{\sqrt{3}}{2}$. Idem pour arctan en 0, 1, $\sqrt{3}$ et $\frac{1}{\sqrt{3}}$.
2. Calculer $\arccos(\cos\frac{7\pi}{3})$. Idem avec $\arcsin(\sin\frac{7\pi}{3})$ et $\arctan(\tan\frac{7\pi}{3})$ (attention aux intervalles !)
3. Calculer $\cos(\arctan x)$, $\cos(\arcsin x)$, $\tan(\arcsin x)$.
4. Calculer la dérivée de $f(x) = \arctan\left(\frac{x}{\sqrt{1-x^2}}\right)$. En déduire que $f(x) = \arcsin x$, pour tout $x \in]-1, 1[$.
5. Montrer que $\arccos x + \arcsin x = \frac{\pi}{2}$, pour tout $x \in [-1, 1]$.

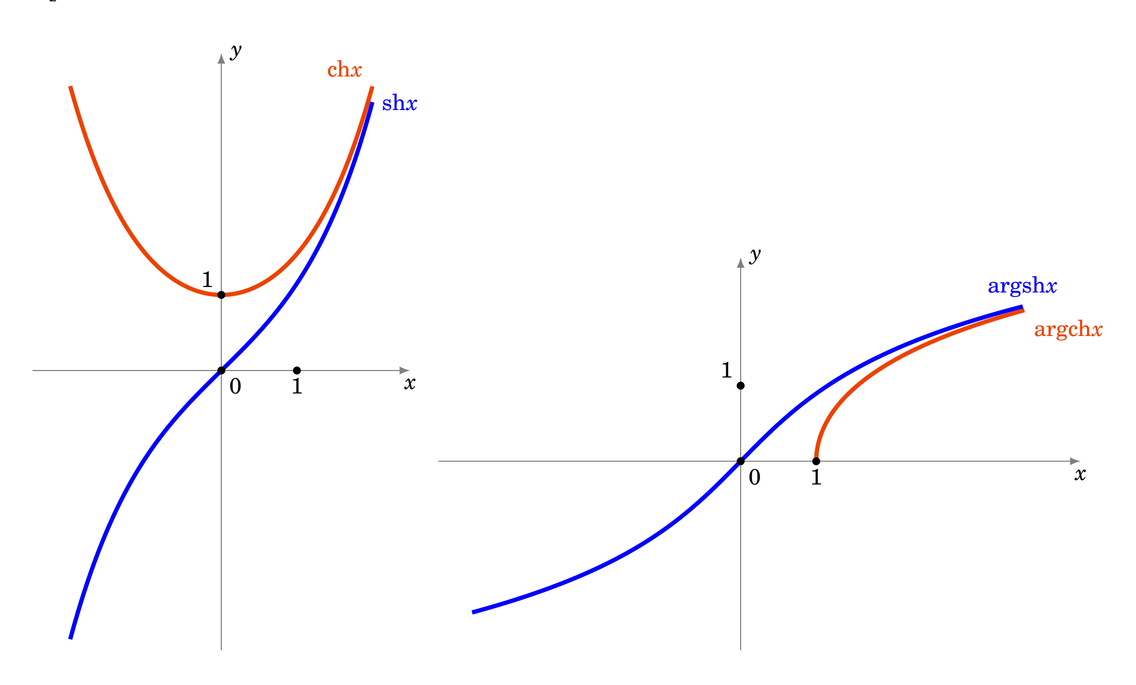
3. Fonctions hyperboliques et hyperboliques inverses

3.1. Cosinus hyperbolique et son inverse

Pour $x \in \mathbb{R}$, le ***cosinus hyperbolique*** est :

$$\operatorname{ch} x = \frac{e^x + e^{-x}}{2}$$

La restriction $\operatorname{ch}_| : [0, +\infty[\to [1, +\infty[$ est une bijection. Sa bijection réciproque est $\operatorname{Argch} : [1, +\infty[\to [0, +\infty[$.



3.2. Sinus hyperbolique et son inverse

Pour $x \in \mathbb{R}$, le ***sinus hyperbolique*** est :

$$\operatorname{sh} x = \frac{e^x - e^{-x}}{2}$$

$\operatorname{sh} : \mathbb{R} \to \mathbb{R}$ est une fonction continue, dérivable, strictement croissante vérifiant $\lim_{x\to-\infty} \operatorname{sh} x = -\infty$ et $\lim_{x\to+\infty} \operatorname{sh} x = +\infty$, c'est donc une bijection. Sa bijection réciproque est $\operatorname{Argsh} : \mathbb{R} \to \mathbb{R}$.

Proposition 68

- $\operatorname{ch}^2 x - \operatorname{sh}^2 x = 1$.
- $\operatorname{ch}' x = \operatorname{sh} x$, $\operatorname{sh}' x = \operatorname{ch} x$.
- $\operatorname{Argsh} : \mathbb{R} \to \mathbb{R}$ est strictement croissante et continue.
- Argsh est dérivable et $\operatorname{Argsh}' x = \frac{1}{\sqrt{x^2+1}}$.
- $\operatorname{Argsh} x = \ln\left(x + \sqrt{x^2+1}\right)$.

Démonstration

- $\operatorname{ch}^2 x - \operatorname{sh}^2 x = \frac{1}{4}\left[(e^x + e^{-x})^2 - (e^x - e^{-x})^2\right] = \frac{1}{4}\left[(e^{2x} + 2 + e^{-2x}) - (e^{2x} - 2 + e^{-2x})\right] = 1$.
- $\frac{d}{dx}(\operatorname{ch} x) = \frac{d}{dx}\frac{e^x + e^{-x}}{2} = \frac{e^x - e^{-x}}{2} = \operatorname{sh} x$. Idem pour la dérivée de $\operatorname{sh} x$.
- Car c'est la réciproque de sh.
- Comme la fonction $x \mapsto \operatorname{sh}' x$ ne s'annule pas sur $\mathbb{R}$ alors la fonction Argsh est dérivable sur $\mathbb{R}$. On calcule la dérivée par dérivation de l'égalité $\operatorname{sh}(\operatorname{Argsh} x) = x$:

$$\operatorname{Argsh}' x = \frac{1}{\operatorname{ch}(\operatorname{Argsh} x)} = \frac{1}{\sqrt{\operatorname{sh}^2(\operatorname{Argsh} x) + 1}} = \frac{1}{\sqrt{x^2 + 1}}$$

- Notons $f(x) = \ln\left(x + \sqrt{x^2 + 1}\right)$ alors

$$f'(x) = \frac{1 + \frac{x}{\sqrt{x^2+1}}}{x + \sqrt{x^2 + 1}} = \frac{1}{\sqrt{x^2 + 1}} = \operatorname{Argsh}' x$$

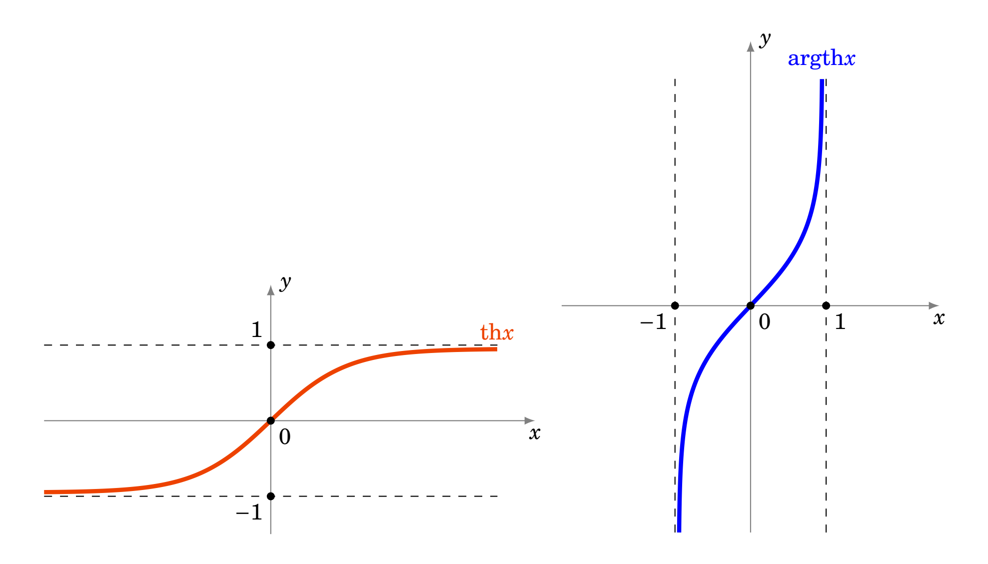
Comme de plus $f(0) = \ln(1) = 0$ et $\operatorname{Argsh} 0 = 0$ (car $\operatorname{sh} 0 = 0$), on en déduit que pour tout $x \in \mathbb{R}$, $f(x) = \operatorname{Argsh} x$.

3.3. Tangente hyperbolique et son inverse

Par définition la ***tangente hyperbolique*** est :

$$\operatorname{th} x = \frac{\operatorname{sh} x}{\operatorname{ch} x}$$

La fonction $\operatorname{th} : \mathbb{R} \to]-1, 1[$ est une bijection, on note $\operatorname{Argth} :]-1, 1[\to \mathbb{R}$ sa bijection réciproque.



3.4. Trigonométrie hyperbolique

$$\operatorname{ch}^2 x - \operatorname{sh}^2 x = 1$$

$$
\begin{aligned}
\operatorname{ch}(a+b) &= \operatorname{ch} a \cdot \operatorname{ch} b + \operatorname{sh} a \cdot \operatorname{sh} b \\
\operatorname{ch}(2a) &= \operatorname{ch}^2 a + \operatorname{sh}^2 a = 2\operatorname{ch}^2 a - 1 = 1 + 2\operatorname{sh}^2 a
\end{aligned}
$$

$$
\begin{aligned}
\operatorname{sh}(a+b) &= \operatorname{sh} a \cdot \operatorname{ch} b + \operatorname{sh} b \cdot \operatorname{ch} a \\
\operatorname{sh}(2a) &= 2\operatorname{sh} a \cdot \operatorname{ch} a
\end{aligned}
$$

$$
\operatorname{th}(a+b) = \frac{\operatorname{th} a + \operatorname{th} b}{1 + \operatorname{th} a \cdot \operatorname{th} b}
$$

$$
\begin{aligned}
\operatorname{ch}' x &= \operatorname{sh} x \\
\operatorname{sh}' x &= \operatorname{ch} x \\
\operatorname{th}' x &= 1 - \operatorname{th}^2 x = \frac{1}{\operatorname{ch}^2 x}
\end{aligned}
$$

$$
\begin{aligned}
\operatorname{Argch}' x &= \frac{1}{\sqrt{x^2-1}} \quad (x > 1) \\
\operatorname{Argsh}' x &= \frac{1}{\sqrt{x^2+1}} \\
\operatorname{Argth}' x &= \frac{1}{1-x^2} \quad (|x| < 1)
\end{aligned}
$$

$$
\begin{aligned}
\operatorname{Argch} x &= \ln\left(x + \sqrt{x^2-1}\right) \quad (x \geqslant 1) \\
\operatorname{Argsh} x &= \ln\left(x + \sqrt{x^2+1}\right) \quad (x \in \mathbb{R}) \\
\operatorname{Argth} x &= \frac{1}{2}\ln\left(\frac{1+x}{1-x}\right) \quad (-1 < x < 1)
\end{aligned}
$$

Mini-exercices

1. Dessiner les courbes paramétrées $t \mapsto (\cos t, \sin t)$ et $t \mapsto (\operatorname{ch} t, \operatorname{sh} t)$. Pourquoi cos et sin s'appellent des fonctions trigonométriques *circulaires* alors que ch et sh sont des fonctions trigonométriques *hyperboliques* ?
2. Prouver par le calcul la formule $\operatorname{ch}(a+b) = \ldots$ En utilisant que $\cos x = \frac{e^{ix}+e^{-ix}}{2}$ retrouver la formule pour $\cos(a+b)$.
3. Résoudre l'équation $\operatorname{sh} x = 3$.
4. Montrer que $\frac{\operatorname{sh}(2x)}{1+\operatorname{ch}(2x)} = \operatorname{th} x$.
5. Calculer les dérivées des fonctions définies par : $\operatorname{th}(1+x^2)$, $\ln(\operatorname{ch} x)$, $\operatorname{Argch}(\exp x)$, $\operatorname{Argth}(\cos x)$.

Auteurs

Arnaud Bodin, Niels Borne, Laura Desideri

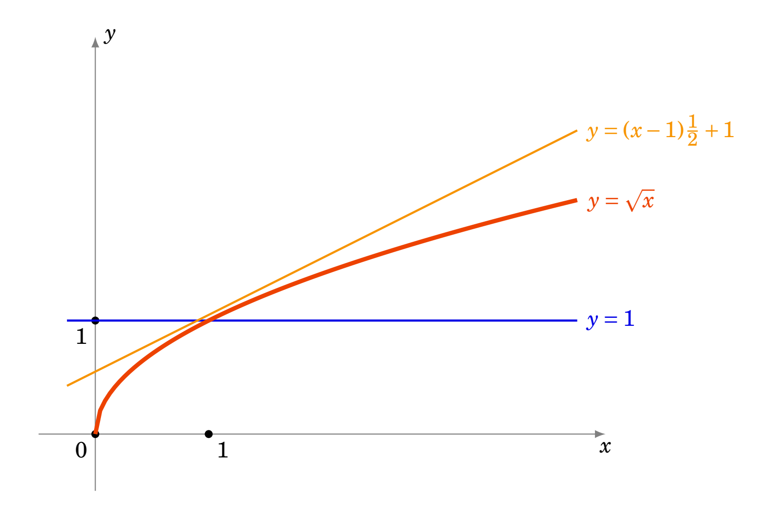
Exo7

10 Dérivée d'une fonction

Vidéo ■ partie 1. Définition
Vidéo ■ partie 2. Calculs
Vidéo ■ partie 3. Extremum local, théorème de Rolle
Vidéo ■ partie 4. Théorème des accroissements finis
Exercices ♦ Fonctions dérivables

Motivation

Nous souhaitons calculer $\sqrt{1{,}01}$ ou du moins en trouver une valeur approchée. Comme $1{,}01$ est proche de 1 et que $\sqrt{1} = 1$ on se doute bien que $\sqrt{1{,}01}$ sera proche de 1. Peut-on être plus précis ? Si l'on appelle f la fonction définie par $f(x) = \sqrt{x}$, alors la fonction f est une fonction continue en $x_0 = 1$. La continuité nous affirme que pour x suffisamment proche de x_0, $f(x)$ est proche de $f(x_0)$. Cela revient à dire que pour x au voisinage de x_0 on approche $f(x)$ par la constante $f(x_0)$.



Nous pouvons faire mieux qu'approcher notre fonction par une droite horizontale ! Essayons avec une droite quelconque. Quelle droite se rapproche le plus du graphe de f autour de x_0 ? Elle doit passer par le point $(x_0, f(x_0))$ et doit «coller» le plus possible au graphe : c'est la tangente au graphe en x_0. Une équation de la tangente est

$$y = (x - x_0)f'(x_0) + f(x_0)$$

où $f'(x_0)$ désigne le nombre dérivé de f en x_0.
On sait que pour $f(x) = \sqrt{x}$, on a $f'(x) = \frac{1}{2\sqrt{x}}$. Une équation de la tangente en $x_0 = 1$ est donc $y = (x-1)\frac{1}{2} + 1$. Et donc pour x proche de 1 on a $f(x) \approx (x-1)\frac{1}{2} + 1$. Qu'est ce que cela donne

pour notre calcul de $\sqrt{1{,}01}$? On pose $x = 1{,}01$ donc $f(x) \approx 1 + \frac{1}{2}(x-1) = 1 + \frac{0{,}01}{2} = 1{,}005$. Et c'est effectivement une très bonne de approximation de $\sqrt{0{,}01} = 1{,}00498\ldots$. En posant $h = x-1$ on peut reformuler notre approximation en : $\sqrt{1+h} \approx 1 + \frac{1}{2}h$ qui est valable pour h proche de 0.
Dans ce chapitre nous allons donc définir ce qu'est la dérivée d'une fonction, et établir les formules des dérivées des fonctions usuelles. Enfin, pour connaître l'erreur des approximations, il nous faudra travailler beaucoup plus afin d'obtenir le théorème des accroissements finis.

1. Dérivée

1.1. Dérivée en un point

Soit I un intervalle ouvert de $\mathbb{R}$ et $f : I \to \mathbb{R}$ une fonction. Soit $x_0 \in I$.

Définition 59

f est ***dérivable en x_0*** si le ***taux d'accroissement*** $\frac{f(x)-f(x_0)}{x-x_0}$ a une limite finie lorsque x tend vers x_0. La limite s'appelle alors le ***nombre dérivé*** de f en x_0 et est noté $f'(x_0)$. Ainsi

$$\boxed{f'(x_0) = \lim_{x\to x_0} \frac{f(x)-f(x_0)}{x-x_0}}$$

Définition 60

f est ***dérivable sur I*** si f est dérivable en tout point $x_0 \in I$. La fonction $x \mapsto f'(x)$ est la ***fonction dérivée*** de f, elle se note f' ou $\frac{df}{dx}$.

Exemple 101

La fonction définie par $f(x) = x^2$ est dérivable en tout point $x_0 \in \mathbb{R}$. En effet :

$$\frac{f(x)-f(x_0)}{x-x_0} = \frac{x^2-x_0^2}{x-x_0} = \frac{(x-x_0)(x+x_0)}{x-x_0} = x + x_0 \xrightarrow[x\to x_0]{} 2x_0.$$

On a même montré que le nombre dérivé de f en x_0 est $2x_0$, autrement dit : $f'(x) = 2x$.

Exemple 102

Montrons que la dérivée de $f(x) = \sin x$ est $f'(x) = \cos x$. Nous allons utiliser les deux assertions suivantes :

$$\frac{\sin x}{x} \xrightarrow[x\to 0]{} 1 \qquad \text{et} \qquad \sin p - \sin q = 2\sin\frac{p-q}{2}\cdot\cos\frac{p+q}{2}.$$

Remarquons déjà que la première assertion prouve $\frac{f(x)-f(0)}{x-0} = \frac{\sin x}{x} \to 1$ et donc f est dérivable en $x_0 = 0$ et $f'(0) = 1$.
Pour x_0 quelconque on écrit :

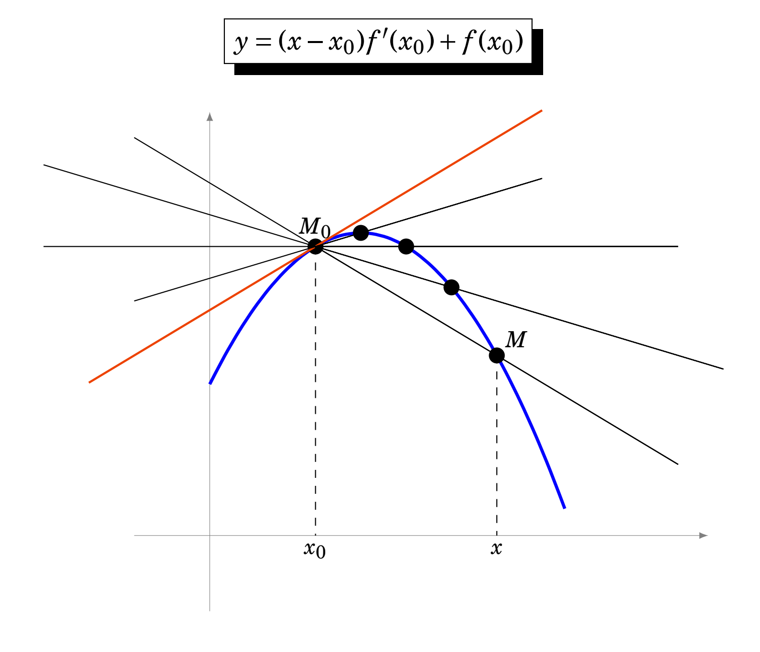
$$\frac{f(x)-f(x_0)}{x-x_0} = \frac{\sin x - \sin x_0}{x-x_0} = \frac{\sin\frac{x-x_0}{2}}{\frac{x-x_0}{2}}\cdot\cos\frac{x+x_0}{2}.$$

Lorsque $x \to x_0$ alors d'une part $\cos\frac{x+x_0}{2} \to \cos x_0$ et d'autre part en posant $u = \frac{x-x_0}{2}$ alors $u \to 0$ et on a $\frac{\sin u}{u} \to 1$. Ainsi $\frac{f(x)-f(x_0)}{x-x_0} \to \cos x_0$ et donc $f'(x) = \cos x$.

1.2. Tangente

La droite qui passe par les points distincts $(x_0, f(x_0))$ et $(x, f(x))$ a pour coefficient directeur $\frac{f(x)-f(x_0)}{x-x_0}$. À la limite on trouve que le coefficient directeur de la tangente est $f'(x_0)$. Une équation de la ***tangente*** au point $(x_0, f(x_0))$ est donc :

$$y = (x - x_0)f'(x_0) + f(x_0)$$



1.3. Autres écritures de la dérivée

Voici deux autres formulations de la dérivabilité de f en x_0.

Proposition 69

- f est dérivable en x_0 si et seulement si $\lim_{h\to 0} \frac{f(x_0+h)-f(x_0)}{h}$ existe et est finie.
- f est dérivable en x_0 si et seulement s'il existe $\ell \in \mathbb{R}$ (qui sera $f'(x_0)$) et une fonction $\varepsilon : I \to \mathbb{R}$ telle que $\varepsilon(x) \xrightarrow[x\to x_0]{} 0$ avec

$$f(x) = f(x_0) + (x - x_0)\ell + (x - x_0)\varepsilon(x).$$

Démonstration

Il s'agit juste de reformuler la définition de $f'(x_0)$. Par exemple, après division par $x - x_0$, la deuxième écriture devient

$$\frac{f(x)-f(x_0)}{x-x_0} = \ell + \varepsilon(x).$$

Proposition 70

Soit I un intervalle ouvert, $x_0 \in I$ et soit $f : I \to \mathbb{R}$ une fonction.

- Si f est dérivable en x_0 alors f est continue en x_0.
- Si f est dérivable sur I alors f est continue sur I.

Démonstration

Supposons f dérivable en x_0 et montrons qu'elle est aussi continue en ce point.
Voici une démonstration concise : partant de l'écriture alternative donnée dans la proposition 69, nous écrivons

$$f(x) = f(x_0) + \underbrace{(x - x_0)\ell}_{\to 0} + \underbrace{(x - x_0)\varepsilon(x)}_{\to 0}.$$

Donc $f(x) \to f(x_0)$ lorsque $x \to x_0$ et ainsi f est continue en x_0.

On reprend cette démonstration sans utiliser les limites mais uniquement la définition de continuité et dérivabilité :
Fixons $\varepsilon' > 0$ et écrivons $f(x) = f(x_0) + (x - x_0)\ell + (x - x_0)\varepsilon(x)$ grâce à la proposition 69, où $\varepsilon(x) \xrightarrow[x \to x_0]{} 0$ et $\ell = f'(x_0)$. Choisissons $\delta > 0$ de sorte qu'il vérifie tous les points suivants :

- $\delta \leqslant 1$
- $\delta|\ell| < \varepsilon'$
- si $|x - x_0| < \delta$ alors $|\varepsilon(x)| < \varepsilon'$ (c'est possible car $\varepsilon(x) \to 0$)

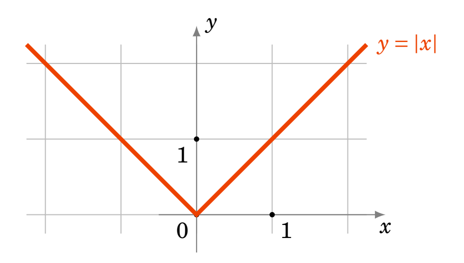
Alors l'égalité ci-dessus devient :

$$\begin{aligned}
\left|f(x) - f(x_0)\right| &= \left|(x - x_0)\ell + (x - x_0)\varepsilon(x)\right| \\
&\leqslant |x - x_0| \cdot |\ell| + |x - x_0| \cdot |\varepsilon(x)| \\
&\leqslant \delta|\ell| \quad + \quad \delta\varepsilon' \qquad \text{pour } |x - x_0| < \delta \\
&\leqslant \varepsilon' + \varepsilon' = 2\varepsilon'
\end{aligned}$$

Nous venons de prouver que si $|x - x_0| < \delta$ alors $\left|f(x) - f(x_0)\right| < 2\varepsilon'$, ce qui exprime exactement que f est continue en x_0.

Remarque

La réciproque est **fausse** : par exemple, la fonction valeur absolue est continue en 0 mais n'est pas dérivable en 0.



En effet, le taux d'accroissement de $f(x) = |x|$ en $x_0 = 0$ vérifie :

$$\frac{f(x) - f(0)}{x - 0} = \frac{|x|}{x} = \begin{cases} +1 & \text{si } x > 0 \\ -1 & \text{si } x < 0 \end{cases}.$$

Il y a bien une limite à droite (qui vaut $+1$), une limite à gauche (qui vaut -1) mais elles ne sont pas égales : il n'y a pas de limite en 0. Ainsi f n'est pas dérivable en $x = 0$.
Cela se lit aussi sur le dessin il y a une demi-tangente à droite, une demi-tangente à gauche mais elles ont des directions différentes.

Mini-exercices

1. Montrer que la fonction $f(x) = x^3$ est dérivable en tout point $x_0 \in \mathbb{R}$ et que $f'(x_0) = 3x_0^2$.
2. Montrer que la fonction $f(x) = \sqrt{x}$ est dérivable en tout point $x_0 > 0$ et que $f'(x_0) = \frac{1}{2\sqrt{x_0}}$.
3. Montrer que la fonction $f(x) = \sqrt{x}$ (qui est continue en $x_0 = 0$) n'est pas dérivable en $x_0 = 0$.
4. Calculer l'équation de la tangente (T_0) à la courbe d'équation $y = x^3 - x^2 - x$ au point d'abscisse $x_0 = 2$. Calculer x_1 afin que la tangente (T_1) au point d'abscisse x_1 soit parallèle à (T_0).
5. Montrer que si une fonction f est paire et dérivable, alors f' est une fonction impaire.

2. Calcul des dérivées

2.1. Somme, produit,...

Proposition 71

Soient $f, g : I \to \mathbb{R}$ deux fonctions dérivables sur I. Alors pour tout $x \in I$:

- $(f+g)'(x) = f'(x) + g'(x)$,
- $(\lambda f)'(x) = \lambda f'(x)$ où λ est un réel fixé,
- $(f \times g)'(x) = f'(x)g(x) + f(x)g'(x)$,
- $\left(\frac{1}{f}\right)'(x) = -\frac{f'(x)}{f(x)^2}$ (si $f(x) \neq 0$),
- $\left(\frac{f}{g}\right)'(x) = \frac{f'(x)g(x) - f(x)g'(x)}{g(x)^2}$ (si $g(x) \neq 0$).

Remarque

Il est plus facile de mémoriser les égalités de fonctions :

$$(f+g)' = f' + g', \quad (\lambda f)' = \lambda f', \quad (f \times g)' = f'g + fg', \quad \left(\frac{1}{f}\right)' = -\frac{f'}{f^2}, \quad \left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}.$$

Démonstration

Prouvons par exemple $(f \times g)' = f'g + fg'$.
Fixons $x_0 \in I$. Nous allons réécrire le taux d'accroissement de $f(x) \times g(x)$:

$$\frac{f(x)g(x) - f(x_0)g(x_0)}{x - x_0} = \frac{f(x) - f(x_0)}{x - x_0} g(x) + \frac{g(x) - g(x_0)}{x - x_0} f(x_0) \xrightarrow[x \to x_0]{} f'(x_0)g(x_0) + g'(x_0)f(x_0).$$

Ceci étant vrai pour tout $x_0 \in I$ la fonction $f \times g$ est dérivable sur I de dérivée $f'g + fg'$.

2.2. Dérivée de fonctions usuelles

Le tableau de gauche est un résumé des principales formules à connaître, x est une variable. Le tableau de droite est celui des compositions (voir paragraphe suivant), u représente une fonction $x \mapsto u(x)$.

Fonction	Dérivée
x^n	$nx^{n-1} \quad (n \in \mathbb{Z})$
$\frac{1}{x}$	$-\frac{1}{x^2}$
$\sqrt{x}$	$\frac{1}{2}\frac{1}{\sqrt{x}}$
x^α	$\alpha x^{\alpha-1} \quad (\alpha \in \mathbb{R})$
e^x	e^x
$\ln x$	$\frac{1}{x}$
$\cos x$	$-\sin x$
$\sin x$	$\cos x$
$\tan x$	$1+\tan^2 x = \frac{1}{\cos^2 x}$

Fonction	Dérivée
u^n	$nu'u^{n-1} \quad (n \in \mathbb{Z})$
$\frac{1}{u}$	$-\frac{u'}{u^2}$
$\sqrt{u}$	$\frac{1}{2}\frac{u'}{\sqrt{u}}$
u^α	$\alpha u'u^{\alpha-1} \quad (\alpha \in \mathbb{R})$
e^u	$u'e^u$
$\ln u$	$\frac{u'}{u}$
$\cos u$	$-u'\sin u$
$\sin u$	$u'\cos u$
$\tan u$	$u'(1+\tan^2 u) = \frac{u'}{\cos^2 u}$

Remarque

- Notez que les formules pour x^n, $\frac{1}{x}$ $\sqrt{x}$ et x^α sont aussi des conséquences de la dérivée de l'exponentielle. Par exemple $x^\alpha = e^{\alpha \ln x}$ et donc

$$\frac{d}{dx}(x^\alpha) = \frac{d}{dx}(e^{\alpha \ln x}) = \alpha\frac{1}{x}e^{\alpha \ln x} = \alpha\frac{1}{x}x^\alpha = \alpha x^{\alpha-1}.$$

- Si vous devez dériver une fonction avec un exposant dépendant de x il faut absolument repasser à la forme exponentielle. Par exemple si $f(x) = 2^x$ alors on réécrit d'abord $f(x) = e^{x\ln 2}$ pour pouvoir calculer $f'(x) = \ln 2 \cdot e^{x \ln 2} = \ln 2 \cdot 2^x$.

2.3. Composition

Proposition 72

Si f est dérivable en x et g est dérivable en $f(x)$ alors $g \circ f$ est dérivable en x de dérivée :

$$\boxed{\big(g \circ f\big)'(x) = g'\big(f(x)\big) \cdot f'(x)}$$

Démonstration

La preuve est similaire à celle ci-dessus pour le produit en écrivant cette fois :

$$\frac{g \circ f(x) - g \circ f(x_0)}{x - x_0} = \frac{g\big(f(x)\big) - g\big(f(x_0)\big)}{f(x) - f(x_0)} \times \frac{f(x) - f(x_0)}{x - x_0} \xrightarrow[x \to x_0]{} g'\big(f(x_0)\big) \times f'(x_0).$$

Exemple 103

Calculons la dérivée de $\ln(1+x^2)$. Nous avons $g(x) = \ln(x)$ avec $g'(x) = \frac{1}{x}$; et $f(x) = 1+x^2$ avec $f'(x) = 2x$. Alors la dérivée de $\ln(1+x^2) = g \circ f(x)$ est

$$\big(g \circ f\big)'(x) = g'\big(f(x)\big) \cdot f'(x) = g'\big(1+x^2\big) \cdot 2x = \frac{2x}{1+x^2}.$$

Corollaire 13

Soit I un intervalle ouvert. Soit $f : I \to J$ dérivable et bijective dont on note $f^{-1} : J \to I$ la bijection réciproque. Si f' ne s'annule pas sur I alors f^{-1} est dérivable et on a pour tout $x \in J$:

$$(f^{-1})'(x) = \frac{1}{f'\big(f^{-1}(x)\big)}$$

Démonstration

Notons $g = f^{-1}$ la bijection réciproque de f. Soit $y_0 \in J$ et $x_0 \in I$ tel que $y_0 = f(x_0)$. Le taux d'accroissement de g en y_0 est :

$$\frac{g(y) - g(y_0)}{y - y_0} = \frac{g(y) - x_0}{f\big(g(y)\big) - f(x_0)}$$

Lorsque $y \to y_0$ alors $g(y) \to g(y_0) = x_0$ et donc ce taux d'accroissement tend vers $\frac{1}{f'(x_0)}$. Ainsi $g'(y_0) = \frac{1}{f'(x_0)}$.

Remarque

Il peut être plus simple de retrouver la formule à chaque fois en dérivant l'égalité

$$f\big(g(x)\big) = x$$

où $g = f^{-1}$ est la bijection réciproque de f.
En effet à droite la dérivée de x est 1 ; à gauche la dérivée de $f\big(g(x)\big) = f \circ g(x)$ est $f'\big(g(x)\big) \cdot g'(x)$.
L'égalité $f\big(g(x)\big) = x$ conduit donc à l'égalité des dérivées :

$$f'\big(g(x)\big) \cdot g'(x) = 1.$$

Mais $g = f^{-1}$ donc

$$(f^{-1})'(x) = \frac{1}{f'\big(f^{-1}(x)\big)}.$$

Exemple 104

Soit $f : \mathbb{R} \to \mathbb{R}$ la fonction définie par $f(x) = x + \exp(x)$. Étudions f en détail.
Tout d'abord :

1. f est dérivable car f est la somme de deux fonctions dérivables. En particulier f est continue.
2. f est strictement croissante car f est la somme de deux fonctions strictement croissante.
3. f est une bijection car $\lim_{x \to -\infty} f(x) = -\infty$ et $\lim_{x \to +\infty} f(x) = +\infty$.
4. $f'(x) = 1 + \exp(x)$ ne s'annule jamais (pour tout $x \in \mathbb{R}$).

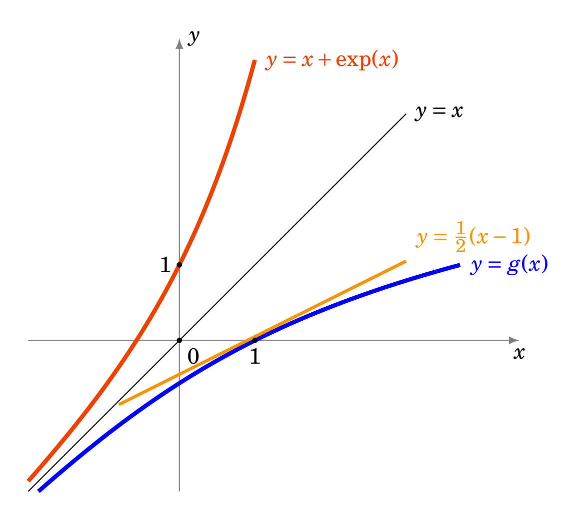
Notons $g = f^{-1}$ la bijection réciproque de f. Même si on ne sait pas a priori exprimer g, on peut malgré tout connaître des informations sur cette fonction : par le corollaire ci-dessus g est dérivable et l'on calcule g' en dérivant l'égalité $f\big(g(x)\big) = x$. Ce qui donne $f'\big(g(x)\big) \cdot g'(x) = 1$

et donc ici

$$g'(x) = \frac{1}{f'\big(g(x)\big)} = \frac{1}{1+\exp\big(g(x)\big)}.$$

Pour cette fonction f particulière on peut préciser davantage : comme $f\big(g(x)\big) = x$ alors $g(x)+\exp\big(g(x)\big) = x$ donc $\exp\big(g(x)\big) = x - g(x)$. Cela conduit à :

$$g'(x) = \frac{1}{1+x-g(x)}.$$



Par exemple $f(0) = 1$ donc $g(1) = 0$ et donc $g'(1) = \frac{1}{2}$. Autrement dit $\big(f^{-1}\big)'(1) = \frac{1}{2}$. L'équation de la tangente au graphe de f^{-1} au point d'abscisse $x_0 = 1$ est donc $y = \frac{1}{2}(x-1)$.

2.4. Dérivées successives

Soit $f : I \to \mathbb{R}$ une fonction dérivable et soit f' sa dérivée. Si la fonction $f' : I \to \mathbb{R}$ est aussi dérivable on note $f'' = (f')'$ la ***dérivée seconde*** de f. Plus généralement on note :

$$f^{(0)} = f, \quad f^{(1)} = f', \quad f^{(2)} = f'' \quad \text{et} \quad f^{(n+1)} = \big(f^{(n)}\big)'$$

Si la ***dérivée n-ième*** $f^{(n)}$ existe on dit que f est ***n fois dérivable***.

Théorème 25. Formule de Leibniz

$$\big(f\cdot g\big)^{(n)} = f^{(n)}\cdot g + \binom{n}{1} f^{(n-1)}\cdot g^{(1)} + \cdots + \binom{n}{k} f^{(n-k)}\cdot g^{(k)} + \cdots + f\cdot g^{(n)}$$

Autrement dit :

$$\big(f\cdot g\big)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(n-k)}\cdot g^{(k)}.$$

La démonstration est similaire à celle de la formule du binôme de Newton et les coefficients que l'on obtient sont les mêmes.

Exemple 105

- Pour $n = 1$ on retrouve $(f \cdot g)' = f'g + fg'$.
- Pour $n = 2$, on a $(f \cdot g)'' = f''g + 2f'g' + fg''$.

Exemple 106

Calculons les dérivées n-ième de $\exp(x) \cdot (x^2 + 1)$ pour tout $n \geqslant 0$. Notons $f(x) = \exp(x)$ alors $f'(x) = \exp(x)$, $f''(x) = \exp(x)$,...,$f^{(k)}(x) = \exp(x)$. Notons $g(x) = x^2 + 1$ alors $g'(x) = 2x$, $g''(x) = 2$ et pour $k \geqslant 3$, $g^{(k)}(x) = 0$.
Appliquons la formule de Leibniz :

$$\big(f \cdot g\big)^{(n)}(x) = f^{(n)}(x) \cdot g(x) + \binom{n}{1} f^{(n-1)}(x) \cdot g^{(1)}(x) + \binom{n}{2} f^{(n-2)}(x) \cdot g^{(2)}(x) + \binom{n}{3} f^{(n-3)}(x) \cdot g^{(3)}(x) + \cdots$$

On remplace $f^{(k)}(x) = \exp(x)$ et on sait que $g^{(3)}(x)$, $g^{(4)}(x) = 0, \ldots$ Donc cette somme ne contient que les trois premiers termes :

$$\big(f \cdot g\big)^{(n)}(x) = \exp(x) \cdot (x^2 + 1) + \binom{n}{1} \exp(x) \cdot 2x + \binom{n}{2} \exp(x) \cdot 2.$$

Que l'on peut aussi écrire :

$$\big(f \cdot g\big)^{(n)}(x) = \exp(x) \cdot \Big(x^2 + 2nx + \frac{n(n-1)}{2} + 1\Big).$$

Mini-exercices

1. Calculer les dérivées des fonctions suivantes : $f_1(x) = x \ln x$, $f_2(x) = \sin \frac{1}{x}$, $f_3(x) = \sqrt{1 + \sqrt{1 + x^2}}$, $f_4(x) = \big(\ln(\frac{1+x}{1-x})\big)^{\frac{1}{3}}$, $f_5(x) = x^x$, $f_6(x) = \arctan x + \arctan \frac{1}{x}$.
2. On note $\Delta(f) = \frac{f'}{f}$. Calculer $\Delta(f \times g)$.
3. Soit $f :]1, +\infty[\to]-1, +\infty[$ définie par $f(x) = x \ln(x) - x$. Montrer que f est une bijection. Notons $g = f^{-1}$. Calculer $g(0)$ et $g'(0)$.
4. Calculer les dérivées successives de $f(x) = \ln(1 + x)$.
5. Calculer les dérivées successives de $f(x) = \ln(x) \cdot x^3$.

3. Extremum local, théorème de Rolle

3.1. Extremum local

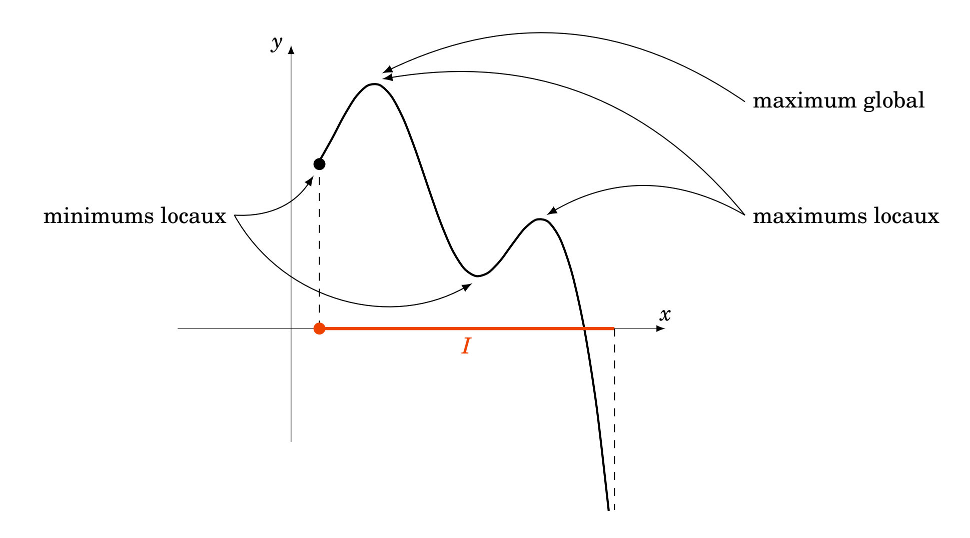
Soit $f : I \to \mathbb{R}$ une fonction définie sur un intervalle I.

Définition 61

- On dit que x_0 est un ***point critique*** de f si $f'(x_0) = 0$.
- On dit que f admet un ***maximum local en*** x_0 (resp. un ***minimum local en*** x_0) s'il existe un intervalle ouvert J contenant x_0 tel que

$$\text{pour tout } x \in I \cap J \quad f(x) \leqslant f(x_0)$$

(resp. $f(x) \geqslant f(x_0)$).
- On dit que f admet un ***extremum local en*** x_0 si f admet un maximum local ou un minimum local en ce point.

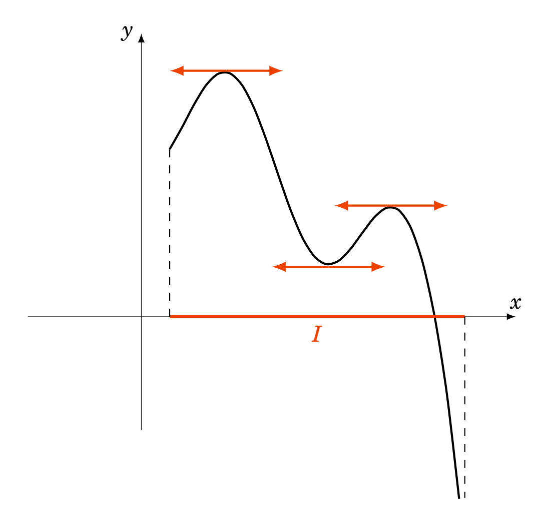


Dire que f a un maximum local en x_0 signifie que $f(x_0)$ est la plus grande des valeurs $f(x)$ pour les x proches de x_0. On dit que $f : I \to \mathbb{R}$ admet un ***maximum global*** en x_0 si pour toutes les autres valeurs $f(x)$, $x \in I$ on a $f(x) \leqslant f(x_0)$ (on ne regarde donc pas seulement les $f(x)$ pour x proche de x_0). Bien sûr un maximum global est aussi un maximum local, mais la réciproque est fausse.

Théorème 26

Soit I un intervalle ouvert et $f : I \to \mathbb{R}$ une fonction dérivable. Si f admet un maximum local (ou un minimum local) en x_0 alors $f'(x_0) = 0$.

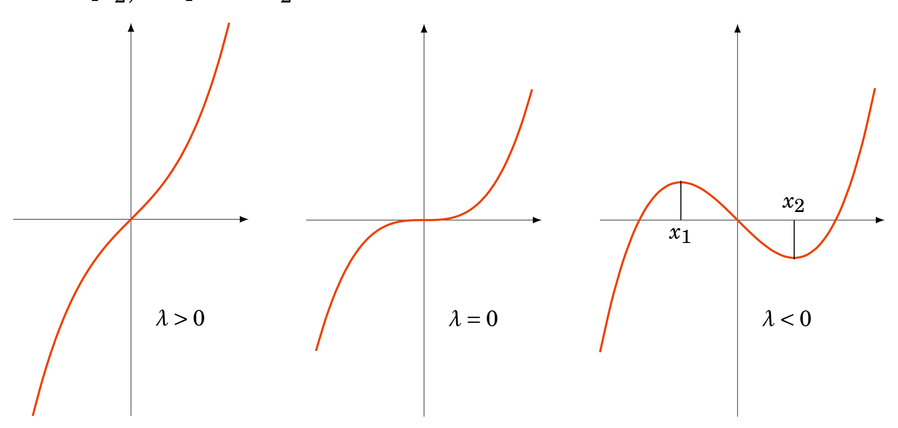
En d'autres termes, un maximum local (ou un minimum local) x_0 est toujours un point critique. Géométriquement, au point $(x_0, f(x_0))$ la tangente au graphe est horizontale.



Exemple 107

Étudions les extremums de la fonction f_λ définie par $f_\lambda(x) = x^3 + \lambda x$ en fonction du paramètre $\lambda \in \mathbb{R}$. La dérivée est $f'_\lambda(x) = 3x^2 + \lambda$. Si x_0 est un extremum local alors $f'_\lambda(x_0) = 0$.

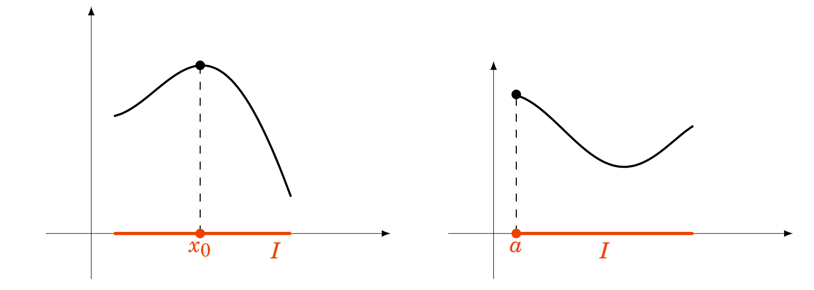
- Si $\lambda > 0$ alors $f'_\lambda(x) > 0$ et ne s'annule jamais il n'y a pas de points critiques donc pas non plus d'extremums. En anticipant sur la suite : f_λ est strictement croissante sur $\mathbb{R}$.
- Si $\lambda = 0$ alors $f'_\lambda(x) = 3x^2$. Le seul point critique est $x_0 = 0$. Mais ce n'est ni un maximum local, ni un minimum local. En effet si $x < 0$, $f_0(x) < 0 = f_0(0)$ et si $x > 0$, $f_0(x) > 0 = f_0(0)$.
- Si $\lambda < 0$ alors $f'_\lambda(x) = 3x^2 - |\lambda| = 3\left(x + \sqrt{\frac{|\lambda|}{3}}\right)\left(x - \sqrt{\frac{|\lambda|}{3}}\right)$. Il y a deux points critiques $x_1 = -\sqrt{\frac{|\lambda|}{3}}$ et $x_2 = +\sqrt{\frac{|\lambda|}{3}}$. En anticipant sur la suite : $f'_\lambda(x) > 0$ sur $]-\infty, x_1[$ et $]x_2, +\infty[$ et $f'_\lambda(x) < 0$ sur $]x_1, x_2[$. Maintenant f_λ est croissante sur $]-\infty, x_1[$, puis décroissante sur $]x_1, x_2[$, donc x_1 est un maximum local. D'autre part f_λ est décroissante sur $]x_1, x_2[$ puis croissante sur $]x_2, +\infty[$ donc x_2 est un minimum local.

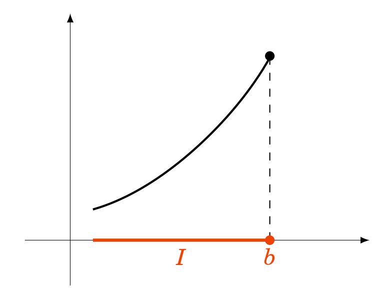


Remarque

1. La réciproque du théorème 26 est fausse. Par exemple la fonction $f : \mathbb{R} \to \mathbb{R}$, définie par $f(x) = x^3$ vérifie $f'(0) = 0$ mais $x_0 = 0$ n'est ni maximum local ni un minimum local.
2. L'intervalle du théorème 26 est ouvert. Pour le cas d'un intervalle fermé, il faut faire attention aux extrémités. Par exemple si $f : [a, b] \to \mathbb{R}$ est une fonction dérivable qui admet un extremum en x_0, alors on est dans l'une des situations suivantes :
   - $x_0 = a$,
   - $x_0 = b$,
   - $x_0 \in]a, b[$ et dans ce cas on a bien $f'(x_0) = 0$ par le théorème 26.

   Aux extrémités on ne peut rien dire pour $f'(a)$ et $f'(b)$, comme le montre les différents maximums sur les dessins suivants.





3. Pour déterminer $\max_{[a,b]} f$ et $\min_{[a,b]} f$ (où $f : [a,b] \to \mathbb{R}$ est une fonction dérivable) il faut comparer les valeurs de f aux différents points critiques et en a et en b.

Démonstration . Preuve du théorème

Supposons que x_0 soit un maximum local de f, soit donc J l'intervalle ouvert de la définition contenant x_0 tel que pour tout $x \in I \cap J$ on a $f(x) \leqslant f(x_0)$.

- Pour $x \in I \cap J$ tel que $x < x_0$ on a $f(x) - f(x_0) \leqslant 0$ et $x - x_0 < 0$ donc $\frac{f(x)-f(x_0)}{x-x_0} \geqslant 0$ et donc à la limite $\lim_{x \to x_0^-} \frac{f(x)-f(x_0)}{x-x_0} \geqslant 0$.
- Pour $x \in I \cap J$ tel que $x > x_0$ on a $f(x) - f(x_0) \leqslant 0$ et $x - x_0 > 0$ donc $\frac{f(x)-f(x_0)}{x-x_0} \leqslant 0$ et donc à la limite $\lim_{x \to x_0^+} \frac{f(x)-f(x_0)}{x-x_0} \leqslant 0$.

Or f est dérivable en x_0 donc

$$\lim_{x \to x_0^-} \frac{f(x)-f(x_0)}{x-x_0} = \lim_{x \to x_0^+} \frac{f(x)-f(x_0)}{x-x_0} = f'(x_0).$$

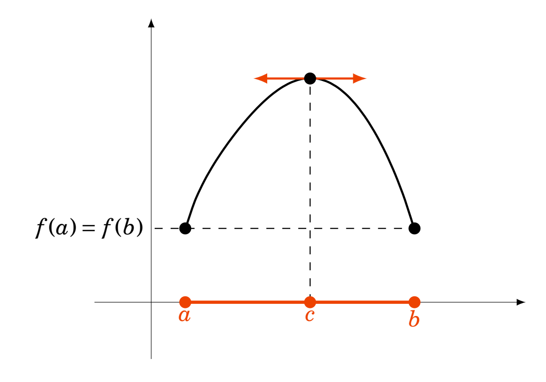
La première limite est positive, la seconde est négative, la seule possibilité est que $f'(x_0) = 0$.

3.2. Théorème de Rolle

Théorème 27. Théorème de Rolle

Soit $f : [a,b] \to \mathbb{R}$ telle que
- f est continue sur $[a,b]$,
- f est dérivable sur $]a,b[$,
- $f(a) = f(b)$.

Alors il existe $c \in]a,b[$ tel que $f'(c) = 0$.



Interprétation géométrique : il existe au moins un point du graphe de f où la tangente est horizontale.

Démonstration

Tout d'abord, si f est constante sur $[a,b]$ alors n'importe quel $c \in]a,b[$ convient. Sinon il existe $x_0 \in [a,b]$ tel que $f(x_0) \neq f(a)$. Supposons par exemple $f(x_0) > f(a)$. Alors f est continue sur l'intervalle fermé et borné $[a,b]$, donc elle admet un maximum en un point $c \in [a,b]$. Mais $f(c) \geqslant f(x_0) > f(a)$ donc $c \neq a$. De même comme $f(a) = f(b)$ alors $c \neq b$. Ainsi $c \in]a,b[$. En c, f est donc dérivable et admet un maximum (local) donc $f'(c) = 0$.

Exemple 108

Soit $P(X) = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)$ un polynôme ayant n racines réelles différentes : $\alpha_1 < \alpha_2 < \cdots < \alpha_n$.

1. *Montrons que P' a $n-1$ racines distinctes.*

   On considère P comme une fonction polynomiale $x \mapsto P(x)$. P est une fonction continue et dérivable sur $\mathbb{R}$. Comme $P(\alpha_1) = 0 = P(\alpha_2)$ alors par le théorème de Rolle il existe $c_1 \in]\alpha_1, \alpha_2[$ tel que $P'(c_1) = 0$. Plus généralement, pour $1 \leqslant k \leqslant n-1$, comme $P(\alpha_k) = 0 = P(\alpha_{k+1})$ alors le théorème de Rolle implique l'existence de $c_k \in]\alpha_k, \alpha_{k+1}[$ tel que $P'(c_k) = 0$. Nous avons bien trouvé $n-1$ racines de P' : $c_1 < c_2 < \cdots < c_{n-1}$. Comme P' est un polynôme de degré $n-1$, toutes ses racines sont réelles et distinctes.

2. *Montrons que $P + P'$ a $n-1$ racines distinctes.*

   L'astuce consiste à considérer la fonction auxiliaire $f(x) = P(x)\exp x$. f est une fonction continue et dérivable sur $\mathbb{R}$. f s'annule comme P en $\alpha_1, \ldots, \alpha_n$.

   La dérivée de f est $f'(x) = \big(P(x) + P'(x)\big)\exp x$. Donc par le théorème de Rolle, pour chaque $1 \leqslant k \leqslant n-1$, comme $f(\alpha_k) = 0 = f(\alpha_{k+1})$ alors il existe $\gamma_k \in]\alpha_k, \alpha_{k+1}[$ tel que $f'(\gamma_k) = 0$. Mais comme la fonction exponentielle ne s'annule jamais alors $(P + P')(\gamma_k) = 0$. Nous avons bien trouvé $n-1$ racines distinctes de $P + P'$: $\gamma_1 < \gamma_2 < \cdots < \gamma_{n-1}$.

3. *Déduisons-en que $P + P'$ a toutes ses racines réelles.*

   $P + P'$ est un polynôme à coefficients réels qui admet $n-1$ racines réelles. Donc $(P + P')(X) = (X - \gamma_1)\cdots(X - \gamma_{n-1})Q(X)$ où $Q(x) = X - \gamma_n$ est un polynôme de degré 1. Comme $P + P'$ est à coefficients réels et que les γ_i sont aussi réels, ainsi $\gamma_n \in \mathbb{R}$. Ainsi on a obtenu une n-ième racine réelle γ_n (pas nécessairement distincte des autres γ_i).

Mini-exercices

1. Dessiner le graphe de fonctions vérifiant : f_1 admet deux minimums locaux et un maximum local ; f_2 admet un minimum local qui n'est pas global et un maximum local qui est global ; f_3 admet une infinité d'extremum locaux ; f_4 n'admet aucun extremum local.
2. Calculer en quel point la fonction $f(x) = ax^2 + bx + c$ admet un extremum local.
3. Soit $f : [0,2] \to \mathbb{R}$ une fonction deux fois dérivable telle que $f(0) = f(1) = f(2) = 0$. Montrer qu'il existe c_1, c_2 tels que $f'(c_1) = 0$ et $f'(c_2) = 0$. Montrer qu'il existe c_3 tel que $f''(c_3) = 0$.
4. Montrer que chacune des trois hypothèses du théorème de Rolle est nécessaire.

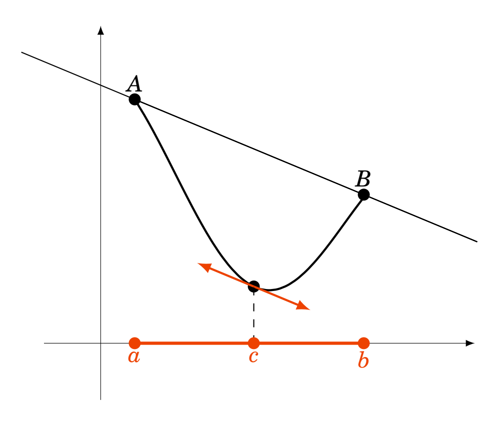
4. Théorème des accroissements finis

4.1. Théorème des accroissements finis

Théorème 28. Théorème des accroissements finis

Soit $f:[a,b]\to\mathbb{R}$ une fonction continue sur $[a,b]$ et dérivable sur $]a,b[$. Il existe $c\in]a,b[$ tel que

$$f(b)-f(a)=f'(c)(b-a)$$



Interprétation géométrique : il existe au moins un point du graphe de f où la tangente est parallèle à la droite (AB) où $A=(a,f(a))$ et $B=(b,f(b))$.

Démonstration

Posons $\ell=\frac{f(b)-f(a)}{b-a}$ et $g(x)=f(x)-\ell\cdot(x-a)$. Alors $g(a)=f(a)$, $g(b)=f(b)-\frac{f(b)-f(a)}{b-a}\cdot(b-a)=f(a)$. Par le théorème de Rolle, il existe $c\in]a,b[$ tel que $g'(c)=0$. Or $g'(x)=f'(x)-\ell$. Ce qui donne $f'(c)=\frac{f(b)-f(a)}{b-a}$.

4.2. Fonction croissante et dérivée

Corollaire 14

Soit $f:[a,b]\to\mathbb{R}$ une fonction continue sur $[a,b]$ et dérivable sur $]a,b[$.

1. $\forall x\in]a,b[\quad f'(x)\geqslant 0 \iff f$ est croissante ;
2. $\forall x\in]a,b[\quad f'(x)\leqslant 0 \iff f$ est décroissante ;
3. $\forall x\in]a,b[\quad f'(x)=0 \iff f$ est constante ;
4. $\forall x\in]a,b[\quad f'(x)>0 \implies f$ est strictement croissante ;
5. $\forall x\in]a,b[\quad f'(x)<0 \implies f$ est strictement décroissante.

Remarque

La réciproque au point (4) (et aussi au (5)) est fausse. Par exemple la fonction $x\mapsto x^3$ est strictement croissante et pourtant sa dérivée s'annule en 0.

Démonstration

Prouvons par exemple (1).

Sens $\Longrightarrow$. Supposons d'abord la dérivée positive. Soient $x, y \in]a, b[$ avec $x \leqslant y$. Alors par le théorème des accroissements finis, il existe $c \in]x, y[$ tel que $f(x) - f(y) = f'(c)(x - y)$. Mais $f'(c) \geqslant 0$ et $x - y \leqslant 0$ donc $f(x) - f(y) \leqslant 0$. Cela implique que $f(x) \leqslant f(y)$. Ceci étant vrai pour tout x, y alors f est croissante.

Sens $\Longleftarrow$. Réciproquement, supposons que f est croissante. Fixons $x \in]a, b[$. Pour tout $y > x$ nous avons $y - x > 0$ et $f(y) - f(x) \geqslant 0$, ainsi le taux d'accroissement vérifie $\frac{f(y)-f(x)}{y-x} \geqslant 0$. À la limite, quand $y \to x$, ce taux d'accroissement tend vers la dérivée de f en x et donc $f'(x) \geqslant 0$.

4.3. Inégalité des accroissements finis

Corollaire 15. Inégalité des accroissements finis

Soit $f : I \to \mathbb{R}$ une fonction dérivable sur un intervalle I ouvert. S'il existe une constante M tel que pour tout $x \in I$, $\left|f'(x)\right| \leqslant M$ alors

$$\boxed{\forall x, y \in I \qquad \left|f(x) - f(y)\right| \leqslant M|x - y|}$$

Démonstration

Fixons $x, y \in I$, il existe alors $c \in]x, y[$ ou $]y, x[$ tel que $f(x) - f(y) = f'(c)(x - y)$ et comme $|f'(c)| \leqslant M$ alors $\left|f(x) - f(y)\right| \leqslant M|x - y|$.

Exemple 109

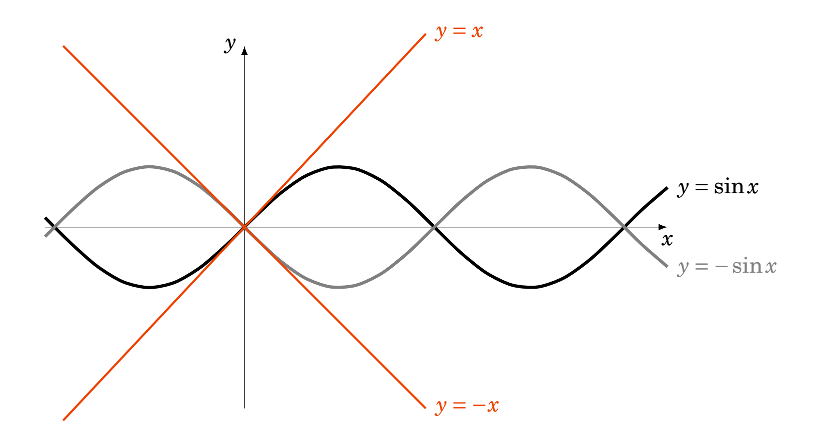
Soit $f(x) = \sin(x)$. Comme $f'(x) = \cos x$ alors $|f'(x)| \leqslant 1$ pour tout $x \in \mathbb{R}$. L'inégalité des accroissements finis s'écrit alors :

$$\text{pour tous } x, y \in \mathbb{R} \qquad |\sin x - \sin y| \leqslant |x - y|.$$

En particulier si l'on fixe $y = 0$ alors on obtient

$$\boxed{|\sin x| \leqslant |x|}$$

ce qui est particulièrement intéressant pour x proche de 0.



4.4. Règle de l'Hospital

Corollaire 16. Règle de l'Hospital

Soient $f,g : I \to \mathbb{R}$ deux fonctions dérivables et soit $x_0 \in I$. On suppose que

- $f(x_0) = g(x_0) = 0$,
- $\forall x \in I \setminus \{x_0\} \quad g'(x) \neq 0$.

$$\text{Si} \quad \lim_{x \to x_0} \frac{f'(x)}{g'(x)} = \ell \quad (\in \mathbb{R}) \quad \text{alors} \quad \lim_{x \to x_0} \frac{f(x)}{g(x)} = \ell.$$

Démonstration

Fixons $a \in I \setminus \{x_0\}$ avec par exemple $a < x_0$. Soit $h : I \to \mathbb{R}$ définie par $h(x) = g(a)f(x) - f(a)g(x)$. Alors

- h est continue sur $[a, x_0] \subset I$,
- h est dérivable sur $]a, x_0[$,
- $h(x_0) = h(a) = 0$.

Donc par le théorème de Rolle il existe $c_a \in]a, x_0[$ tel que $h'(c_a) = 0$.
Or $h'(x) = g(a)f'(x) - f(a)g'(x)$ donc $g(a)f'(c_a) - f(a)g'(c_a) = 0$. Comme g' ne s'annule pas sur $I \setminus \{x_0\}$ cela conduit à $\frac{f(a)}{g(a)} = \frac{f'(c_a)}{g'(c_a)}$. Comme $a < c_a < x_0$ lorsque l'on fait tendre a vers x_0 on obtient $c_a \to x_0$. Cela implique

$$\lim_{a \to x_0} \frac{f(a)}{g(a)} = \lim_{a \to x_0} \frac{f'(c_a)}{g'(c_a)} = \lim_{c_a \to x_0} \frac{f'(c_a)}{g'(c_a)} = \ell.$$

Exemple 110

Calculer la limite en 1 de $\frac{\ln(x^2+x-1)}{\ln(x)}$. On vérifie que :

- $f(x) = \ln(x^2 + x - 1)$, $f(1) = 0$, $f'(x) = \frac{2x+1}{x^2+x-1}$,
- $g(x) = \ln(x)$, $g(1) = 0$, $g'(x) = \frac{1}{x}$,
- Prenons $I =]0, 1]$, $x_0 = 1$, alors g' ne s'annule pas sur $I \setminus \{x_0\}$.

$$\frac{f'(x)}{g'(x)} = \frac{2x+1}{x^2+x-1} \times x = \frac{2x^2+x}{x^2+x-1} \xrightarrow[x \to 1]{} 3.$$

Donc

$$\frac{f(x)}{g(x)} \xrightarrow[x \to 1]{} 3.$$

Mini-exercices

1. Soit $f(x) = \frac{x^3}{3} + \frac{x^2}{2} - 2x + 2$. Étudier la fonction f. Tracer son graphe. Montrer que f admet un minimum local et un maximum local.
2. Soit $f(x) = \sqrt{x}$. Appliquer le théorème des accroissements finis sur l'intervalle $[100, 101]$. En déduire l'encadrement $10 + \frac{1}{22} \leqslant \sqrt{101} \leqslant 10 + \frac{1}{20}$.
3. Appliquer le théorème des accroissements finis pour montrer que $\ln(1+x) - \ln(x) < \frac{1}{x}$ (pour tout $x > 0$).
4. Soit $f(x) = e^x$. Que donne l'inégalité des accroissements finis sur $[0, x]$?
5. Appliquer la règle de l'Hospital pour calculer les limites suivantes (quand $x \to 0$) :

$$\frac{x}{(1+x)^n-1}\ ;\ \frac{\ln(x+1)}{\sqrt{x}}\ ;\ \frac{1-\cos x}{\tan x}\ ;\ \frac{x-\sin x}{x^3}.$$

Auteurs

Arnaud Bodin
Niels Borne
Laura Desideri



11 Zéros des fonctions

Vidéo ■ partie 1. La dichotomie
Vidéo ■ partie 2. La méthode de la sécante
Vidéo ■ partie 3. La méthode de Newton

Dans ce chapitre nous allons appliquer toutes les notions précédentes sur les suites et les fonctions, à la recherche des zéros des fonctions. Plus précisément, nous allons voir trois méthodes afin de trouver des approximations des solutions d'une équation du type $(f(x) = 0)$.

1. La dichotomie

1.1. Principe de la dichotomie

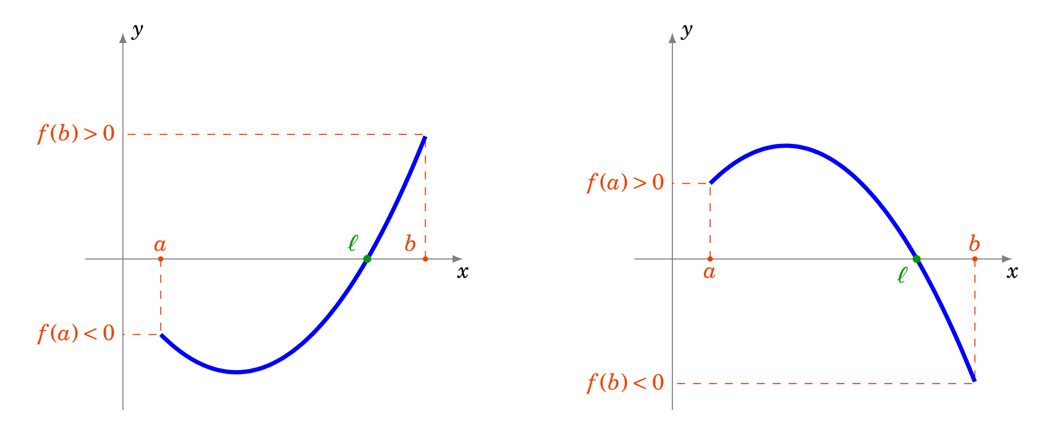
Le principe de dichotomie repose sur la version suivante du ***théorème des valeurs intermédiaires*** :

Théorème 29

Soit $f : [a, b] \to \mathbb{R}$ une fonction continue sur un segment.

$$\text{Si } f(a) \cdot f(b) \leqslant 0, \text{ alors il existe } \ell \in [a, b] \text{ tel que } f(\ell) = 0.$$

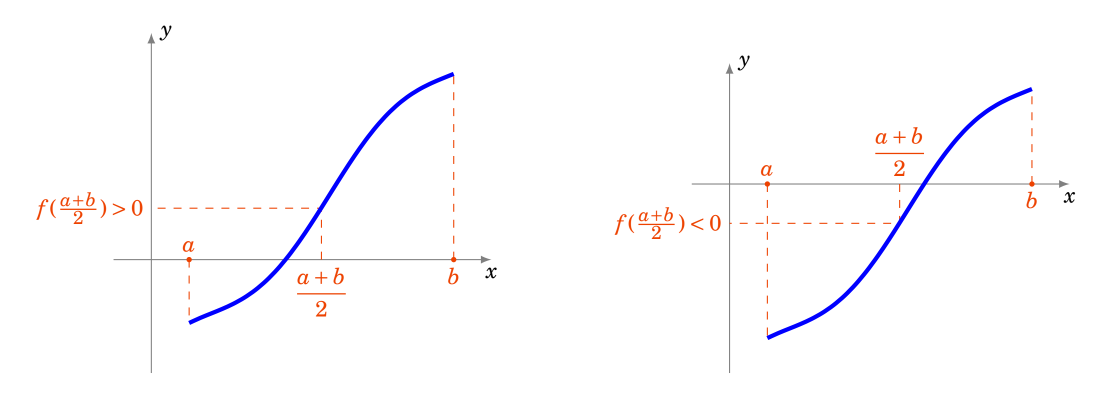
La condition $f(a) \cdot f(b) \leqslant 0$ signifie que $f(a)$ et $f(b)$ sont de signes opposés (ou que l'un des deux est nul). L'hypothèse de continuité est essentielle !



Ce théorème affirme qu'il existe au moins une solution de l'équation $(f(x) = 0)$ dans l'intervalle $[a, b]$. Pour le rendre effectif, et trouver une solution (approchée) de l'équation $(f(x) = 0)$, il s'agit maintenant de l'appliquer sur un intervalle suffisamment petit. On va voir que cela permet d'obtenir un ℓ solution de l'équation $(f(x) = 0)$ comme la limite d'une suite.

Voici comment construire une suite d'intervalles emboîtés, dont la longueur tend vers 0, et contenant chacun une solution de l'équation $(f(x)=0)$.
On part d'une fonction $f : [a,b] \to \mathbb{R}$ continue, avec $a<b$, et $f(a)\cdot f(b) \leqslant 0$.
Voici la première étape de la construction : on regarde le signe de la valeur de la fonction f appliquée au point milieu $\frac{a+b}{2}$.

- Si $f(a)\cdot f(\frac{a+b}{2}) \leqslant 0$, alors il existe $c \in [a, \frac{a+b}{2}]$ tel que $f(c)=0$.
- Si $f(a)\cdot f(\frac{a+b}{2}) > 0$, cela implique que $f(\frac{a+b}{2})\cdot f(b) \leqslant 0$, et alors il existe $c \in [\frac{a+b}{2}, b]$ tel que $f(c)=0$.



Nous avons obtenu un intervalle de longueur moitié dans lequel l'équation $(f(x)=0)$ admet une solution. On itère alors le procédé pour diviser de nouveau l'intervalle en deux.
Voici le processus complet :

- **Au rang 0 :**
  On pose $a_0 = a$, $b_0 = b$. Il existe une solution x_0 de l'équation $(f(x)=0)$ dans l'intervalle $[a_0, b_0]$.
- **Au rang 1 :**
  - Si $f(a_0)\cdot f(\frac{a_0+b_0}{2}) \leqslant 0$, alors on pose $a_1 = a_0$ et $b_1 = \frac{a_0+b_0}{2}$,
  - sinon on pose $a_1 = \frac{a_0+b_0}{2}$ et $b_1 = b$.
  - Dans les deux cas, il existe une solution x_1 de l'équation $(f(x)=0)$ dans l'intervalle $[a_1, b_1]$.
- ...
- **Au rang n :** supposons construit un intervalle $[a_n, b_n]$, de longueur $\frac{b-a}{2^n}$, et contenant une solution x_n de l'équation $(f(x)=0)$. Alors :
  - Si $f(a_n)\cdot f(\frac{a_n+b_n}{2}) \leqslant 0$, alors on pose $a_{n+1} = a_n$ et $b_{n+1} = \frac{a_n+b_n}{2}$,
  - sinon on pose $a_{n+1} = \frac{a_n+b_n}{2}$ et $b_{n+1} = b_n$.
  - Dans les deux cas, il existe une solution x_{n+1} de l'équation $(f(x)=0)$ dans l'intervalle $[a_{n+1}, b_{n+1}]$.

À chaque étape on a

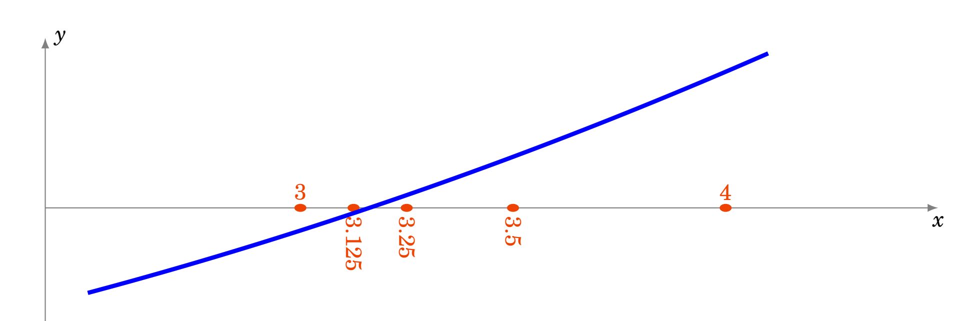
$$a_n \leqslant x_n \leqslant b_n.$$

On arrête le processus dès que $b_n - a_n = \frac{b-a}{2^n}$ est inférieur à la précision souhaitée.
Comme (a_n) est par construction une suite croissante, (b_n) une suite décroissante, et $(b_n - a_n) \to 0$ lorsque $n \to +\infty$, les suites (a_n) et (b_n) sont adjacentes et donc elles admettent une même limite. D'après le théorème des gendarmes, c'est aussi la limite disons ℓ de la suite (x_n). La continuité de f montre que $f(\ell) = \lim_{n\to+\infty} f(x_n) = \lim_{n\to+\infty} 0 = 0$. Donc les suites (a_n) et (b_n) tendent toutes les deux vers ℓ, qui est une solution de l'équation $(f(x)=0)$.

1.2. Résultats numériques pour $\sqrt{10}$

Nous allons calculer une approximation de $\sqrt{10}$. Soit la fonction f définie par $f(x) = x^2 - 10$, c'est une fonction continue sur $\mathbb{R}$ qui s'annule en $\pm\sqrt{10}$. De plus $\sqrt{10}$ est l'unique solution positive de

l'équation ($f(x) = 0$). Nous pouvons restreindre la fonction f à l'intervalle $[3,4]$: en effet $3^2 = 9 \leqslant 10$ donc $3 \leqslant \sqrt{10}$ et $4^2 = 16 \geqslant 10$ donc $4 \geqslant \sqrt{10}$. En d'autre termes $f(3) \leqslant 0$ et $f(4) \geqslant 0$, donc l'équation ($f(x) = 0$) admet une solution dans l'intervalle $[3,4]$ d'après le théorème des valeurs intermédiaires, et par unicité c'est $\sqrt{10}$, donc $\sqrt{10} \in [3,4]$.
Notez que l'on ne choisit pas pour f la fonction $x \mapsto x - \sqrt{10}$ car on ne connaît pas la valeur de $\sqrt{10}$. C'est ce que l'on cherche à calculer !



Voici les toutes premières étapes :

1. On pose $a_0 = 3$ et $b_0 = 4$, on a bien $f(a_0) \leqslant 0$ et $f(b_0) \geqslant 0$. On calcule $\frac{a_0+b_0}{2} = 3,5$ puis $f(\frac{a_0+b_0}{2})$: $f(3,5) = 3,5^2 - 10 = 2,25 \geqslant 0$. Donc $\sqrt{10}$ est dans l'intervalle $[3;3,5]$ et on pose $a_1 = a_0 = 3$ et $b_1 = \frac{a_0+b_0}{2} = 3,5$.
2. On sait donc que $f(a_1) \leqslant 0$ et $f(b_1) \geqslant 0$. On calcule $f(\frac{a_1+b_1}{2}) = f(3,25) = 0,5625 \geqslant 0$, on pose $a_2 = 3$ et $b_2 = 3,25$.
3. On calcule $f(\frac{a_2+b_2}{2}) = f(3,125) = -0,23\ldots \leqslant 0$. Comme $f(b_2) \geqslant 0$ alors cette fois f s'annule sur le second intervalle $[\frac{a_2+b_2}{2}, b_2]$ et on pose $a_3 = \frac{a_2+b_2}{2} = 3,125$ et $b_3 = b_2 = 3,25$.

À ce stade, on a prouvé : $3,125 \leqslant \sqrt{10} \leqslant 3,25$.
Voici la suite des étapes :

$$
\begin{array}{ll}
a_0 = 3 & b_0 = 4 \\
a_1 = 3 & b_1 = 3,5 \\
a_2 = 3 & b_2 = 3,25 \\
a_3 = 3,125 & b_3 = 3,25 \\
a_4 = 3,125 & b_4 = 3,1875 \\
a_5 = 3,15625 & b_5 = 3,1875 \\
a_6 = 3,15625 & b_6 = 3,171875 \\
a_7 = 3,15625 & b_7 = 3,164062\ldots \\
a_8 = 3,16015\ldots & b_8 = 3,164062\ldots
\end{array}
$$

Donc en 8 étapes on obtient l'encadrement :

$$3,160 \leqslant \sqrt{10} \leqslant 3,165$$

En particulier, on vient d'obtenir les deux premières décimales : $\sqrt{10} = 3,16\ldots$

1.3. Résultats numériques pour $(1,10)^{1/12}$

Nous cherchons maintenant une approximation de $(1,10)^{1/12}$. Soit $f(x) = x^{12} - 1,10$. On pose $a_0 = 1$ et $b_0 = 1,1$. Alors $f(a_0) = -0,10 \leqslant 0$ et $f(b_0) = 2,038\ldots \geqslant 0$.

$$\begin{array}{ll} a_0 = 1 & b_0 = 1,10 \\ a_1 = 1 & b_1 = 1,05 \\ a_2 = 1 & b_2 = 1,025 \\ a_3 = 1 & b_3 = 1,0125 \\ a_4 = 1,00625 & b_4 = 1,0125 \\ a_5 = 1,00625 & b_5 = 1,00937\ldots \\ a_6 = 1,00781\ldots & b_6 = 1,00937\ldots \\ a_7 = 1,00781\ldots & b_7 = 1,00859\ldots \\ a_8 = 1,00781\ldots & b_8 = 1,00820\ldots \end{array}$$

Donc en 8 étapes on obtient l'encadrement :

$$1,00781 \leqslant (1,10)^{1/12} \leqslant 1,00821$$

1.4. Calcul de l'erreur

La méthode de dichotomie a l'énorme avantage de fournir un encadrement d'une solution ℓ de l'équation $(f(x) = 0)$. Il est donc facile d'avoir une majoration de l'erreur. En effet, à chaque étape, la taille l'intervalle contenant ℓ est divisée par 2. Au départ, on sait que $\ell \in [a, b]$ (de longueur $b - a$) ; puis $\ell \in [a_1, b_1]$ (de longueur $\frac{b-a}{2}$) ; puis $\ell \in [a_2, b_2]$ (de longueur $\frac{b-a}{4}$) ; ... ; $[a_n, b_n]$ étant de longueur $\frac{b-a}{2^n}$.
Si, par exemple, on souhaite obtenir une approximation de ℓ à 10^{-N} près, comme on sait que $a_n \leqslant \ell \leqslant b_n$, on obtient $|\ell - a_n| \leqslant |b_n - a_n| = \frac{b-a}{2^n}$. Donc pour avoir $|\ell - a_n| \leqslant 10^{-N}$, il suffit de choisir n tel que $\frac{b-a}{2^n} \leqslant 10^{-N}$.
Nous allons utiliser le logarithme décimal :

$$\begin{aligned} \frac{b-a}{2^n} \leqslant 10^{-N} &\iff (b-a)10^N \leqslant 2^n \\ &\iff \log(b-a) + \log(10^N) \leqslant \log(2^n) \\ &\iff \log(b-a) + N \leqslant n \log 2 \\ &\iff n \geqslant \frac{N + \log(b-a)}{\log 2} \end{aligned}$$

Sachant $\log 2 = 0,301\ldots$, si par exemple $b - a \leqslant 1$, voici le nombre d'itérations suffisantes pour avoir une précision de 10^{-N} (ce qui correspond, à peu près, à N chiffres exacts après la virgule).

10^{-10} ($\sim$ 10 décimales)	34 itérations
10^{-100} ($\sim$ 100 décimales)	333 itérations
10^{-1000} ($\sim$ 1000 décimales)	3322 itérations

Il faut entre 3 et 4 itérations supplémentaires pour obtenir une nouvelle décimale.

Remarque

En toute rigueur il ne faut pas confondre précision et nombre de décimales exactes, par exemple $0,999$ est une approximation de $1,000$ à 10^{-3} près, mais aucune décimale après la virgule n'est exacte. En pratique, c'est la précision qui est la plus importante, mais il est plus frappant de parler du nombre de décimales exactes.

1.5. Algorithmes

Voici comment implémenter la dichotomie dans le langage `Python`. Tout d'abord on définit une fonction f (ici par exemple $f(x) = x^2 - 10$) :

Algorithme . dichotomie.py (1)

```
def f(x) :
    return x*x - 10
```

Puis la dichotomie proprement dite : en entrée de la fonction, on a pour variables a, b et n le nombre d'étapes voulues.

Algorithme . dichotomie.py (2)

```
def dicho(a,b,n) :
    for i in range(n) :
        c = (a+b)/2
        if f(a)*f(c) <= 0 :
            b = c
        else :
            a = c
    return a,b
```

Même algorithme, mais avec cette fois en entrée la précision souhaitée :

Algorithme . dichotomie.py (3)

```
def dichobis(a,b,prec) :
    while b-a>prec :
        c = (a+b)/2
        if f(a)*f(c) <= 0 :
            b = c
        else :
            a = c
    return a,b
```

Enfin, voici la version récursive de l'algorithme de dichotomie.

Algorithme . dichotomie.py (4)

```
def dichotomie(a,b,prec) :
    if b-a<=prec :
        return a,b
    else :
        c = (a+b)/2
        if f(a)*f(c) <= 0 :
            return dichotomie(a,c,prec)
        else :
```

```
            return dichotomie(c,b,prec)
```

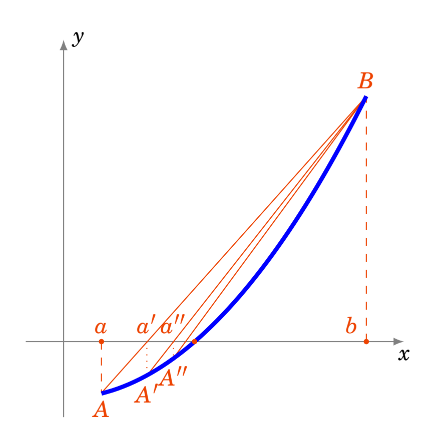
Mini-exercices

1. À la main, calculer un encadrement à $0,1$ près de $\sqrt{3}$. Idem avec $\sqrt[3]{2}$.
2. Calculer une approximation des solutions de l'équation $x^3 + 1 = 3x$.
3. Est-il plus efficace de diviser l'intervalle en 4 au lieu d'en 2 ? (À chaque itération, la dichotomie classique nécessite l'évaluation de f en une nouvelle valeur $\frac{a+b}{2}$ pour une précision améliorée d'un facteur 2.)
4. Écrire un algorithme pour calculer plusieurs solutions de $(f(x) = 0)$.
5. On se donne un tableau trié de taille N, rempli de nombres appartenant à $\{1,\dots,n\}$. Écrire un algorithme qui teste si une valeur k apparaît dans le tableau et en quelle position.

2. La méthode de la sécante

2.1. Principe de la sécante

L'idée de la méthode de la sécante est très simple : pour une fonction f continue sur un intervalle $[a,b]$, et vérifiant $f(a) \leqslant 0$, $f(b) > 0$, on trace le segment $[AB]$ où $A = (a, f(a))$ et $B = (b, f(b))$. Si le segment reste au-dessus du graphe de f alors la fonction s'annule sur l'intervalle $[a', b]$ où $(a', 0)$ est le point d'intersection de la droite (AB) avec l'axe des abscisses. La droite (AB) s'appelle la ***sécante***. On recommence en partant maintenant de l'intervalle $[a', b]$ pour obtenir une valeur a''.



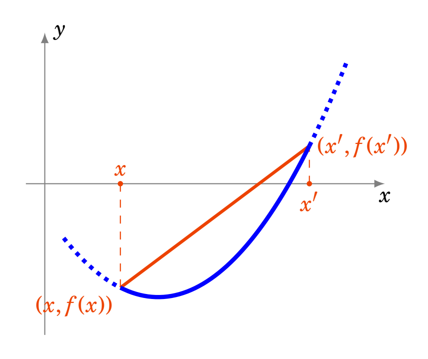
Proposition 73

Soit $f : [a,b] \to \mathbb{R}$ une fonction continue, strictement croissante et convexe telle que $f(a) \leqslant 0$, $f(b) > 0$. Alors la suite définie par

$$a_0 = a \qquad \text{et} \qquad a_{n+1} = a_n - \frac{b - a_n}{f(b) - f(a_n)} f(a_n)$$

est croissante et converge vers la solution ℓ de $(f(x) = 0)$.

L'hypothèse f ***convexe*** signifie exactement que pour tout x, x' dans $[a,b]$ la sécante (ou corde) entre $(x, f(x))$ et $(x', f(x'))$ est au-dessus du graphe de f.



Démonstration

1. Justifions d'abord la construction de la suite récurrente.
   L'équation de la droite passant par les deux points $(a, f(a))$ et $(b, f(b))$ est
   $$y = (x - a)\frac{f(b) - f(a)}{b - a} + f(a)$$
   Cette droite intersecte l'axe des abscisses en $(a', 0)$ qui vérifie donc $0 = (a' - a)\frac{f(b)-f(a)}{b-a} + f(a)$, donc $a' = a - \frac{b-a}{f(b)-f(a)} f(a)$.
2. Croissance de (a_n).
   Montrons par récurrence que $f(a_n) \leqslant 0$. C'est vrai au rang 0 car $f(a_0) = f(a) \leqslant 0$ par hypothèse. Supposons vraie l'hypothèse au rang n. Si $a_{n+1} < a_n$ (un cas qui s'avérera *a posteriori* jamais réalisé), alors comme f est strictement croissante, on a $f(a_{n+1}) < f(a_n)$, et en particulier $f(a_{n+1}) \leqslant 0$. Sinon $a_{n+1} \geqslant a_n$. Comme f est convexe : la sécante entre $(a_n, f(a_n))$ et $(b, f(b))$ est au-dessus du graphe de f. En particulier le point $(a_{n+1}, 0)$ (qui est sur cette sécante par définition a_{n+1}) est au-dessus du point $(a_{n+1}, f(a_{n+1}))$, et donc $f(a_{n+1}) \leqslant 0$ aussi dans ce cas, ce qui conclut la récurrence.
   Comme $f(a_n) \leqslant 0$ et f est croissante, alors par la formule $a_{n+1} = a_n - \frac{b-a_n}{f(b)-f(a_n)} f(a_n)$, on obtient que $a_{n+1} \geqslant a_n$.
3. Convergence de (a_n).
   La suite (a_n) est croissante et majorée par b, donc elle converge. Notons ℓ sa limite. Par continuité $f(a_n) \to f(\ell)$. Comme pour tout n, $f(a_n) \leqslant 0$, on en déduit que $f(\ell) \leqslant 0$. En particulier, comme on suppose $f(b) > 0$, on a $\ell < b$. Comme $a_n \to \ell$, $a_{n+1} \to \ell$, $f(a_n) \to f(\ell)$, l'égalité $a_{n+1} = a_n - \frac{b-a_n}{f(b)-f(a_n)} f(a_n)$ devient à la limite (lorsque $n \to +\infty$) : $\ell = \ell - \frac{b-\ell}{f(b)-f(\ell)} f(\ell)$, ce qui implique $f(\ell) = 0$.
   Conclusion : (a_n) converge vers la solution de $(f(x) = 0)$.

2.2. Résultats numériques pour $\sqrt{10}$

Pour $a = 3$, $b = 4$, $f(x) = x^2 - 10$ voici les résultats numériques, est aussi indiquée une majoration de l'erreur $\varepsilon_n = \sqrt{10} - a_n$ (voir ci-après).

$a_0 = 3$	$\varepsilon_0 \leqslant 0,1666\ldots$
$a_1 = 3,14285714285\ldots$	$\varepsilon_1 \leqslant 0,02040\ldots$
$a_2 = 3,16000000000\ldots$	$\varepsilon_2 \leqslant 0,00239\ldots$
$a_3 = 3,16201117318\ldots$	$\varepsilon_3 \leqslant 0,00028\ldots$
$a_4 = 3,16224648985\ldots$	$\varepsilon_4 \leqslant 3,28\ldots\cdot 10^{-5}$
$a_5 = 3,16227401437\ldots$	$\varepsilon_5 \leqslant 3,84\ldots\cdot 10^{-6}$
$a_6 = 3,16227723374\ldots$	$\varepsilon_6 \leqslant 4,49\ldots\cdot 10^{-7}$
$a_7 = 3,16227761029\ldots$	$\varepsilon_7 \leqslant 5,25\ldots\cdot 10^{-8}$
$a_8 = 3,16227765433\ldots$	$\varepsilon_8 \leqslant 6,14\ldots\cdot 10^{-9}$

2.3. Résultats numériques pour $(1,10)^{1/12}$

Voici les résultats numériques avec une majoration de l'erreur $\varepsilon_n = (1,10)^{1/12} - a_n$, avec $f(x) = x^{12} - 1,10$, $a = 1$ et $b = 1,1$

$a_0 = 1$	$\varepsilon_0 \leqslant 0,0083\ldots$
$a_1 = 1,00467633\ldots$	$\varepsilon_1 \leqslant 0,0035\ldots$
$a_2 = 1,00661950\ldots$	$\varepsilon_2 \leqslant 0,0014\ldots$
$a_3 = 1,00741927\ldots$	$\varepsilon_3 \leqslant 0,00060\ldots$
$a_4 = 1,00774712\ldots$	$\varepsilon_4 \leqslant 0,00024\ldots$
$a_5 = 1,00788130\ldots$	$\varepsilon_5 \leqslant 0,00010\ldots$
$a_6 = 1,00793618\ldots$	$\varepsilon_6 \leqslant 4,14\ldots\cdot 10^{-5}$
$a_7 = 1,00795862\ldots$	$\varepsilon_7 \leqslant 1,69\ldots\cdot 10^{-5}$
$a_8 = 1,00796779\ldots$	$\varepsilon_8 \leqslant 6,92\ldots\cdot 10^{-6}$

2.4. Calcul de l'erreur

La méthode de la sécante fournit l'encadrement $a_n \leqslant l \leqslant b$. Mais comme b est fixe cela ne donne pas d'information exploitable pour $|l - a_n|$. Voici une façon générale d'estimer l'erreur, à l'aide du théorème des accroissements finis.

Proposition 74

Soit $f : I \to \mathbb{R}$ une fonction dérivable et ℓ tel que $f(\ell) = 0$. S'il existe une constante $m > 0$ telle que pour tout $x \in I$, $|f'(x)| \geqslant m$ alors

$$|x - \ell| \leqslant \frac{|f(x)|}{m} \qquad \text{pour tout } x \in I.$$

Démonstration

Par l'inégalité des accroissement finis entre x et ℓ : $|f(x) - f(\ell)| \geqslant m|x - \ell|$ mais $f(\ell) = 0$, d'où la majoration.

Exemple 111. Erreur pour $\sqrt{10}$

Soit $f(x) = x^2 - 10$ et l'intervalle $I = [3,4]$. Alors $f'(x) = 2x$ donc $|f'(x)| \geqslant 6$ sur I. On pose donc $m = 6$, $\ell = \sqrt{10}$, $x = a_n$. On obtient l'estimation de l'erreur :

$$\varepsilon_n = |\ell - a_n| \leqslant \frac{|f(a_n)|}{m} = \frac{|a_n^2 - 10|}{6}$$

Par exemple on a trouvé $a_2 = 3,16... \leqslant 3,17$ donc $\sqrt{10} - a_2 \leqslant \frac{|3,17^2-10|}{6} = 0,489$.
Pour a_8 on a trouvé $a_8 = 3,1622776543347473\ldots$ donc $\sqrt{10} - a_8 \leqslant \frac{|a_8^2-10|}{6} = 6,14\ldots \cdot 10^{-9}$. On a en fait 7 décimales exactes après la virgule.

Dans la pratique, voici le nombre d'itérations suffisantes pour avoir une précision de 10^{-n} pour cet exemple. Grosso-modo, une itération de plus donne une décimale supplémentaire.

10^{-10} ($\sim$ 10 décimales)	10 itérations
10^{-100} ($\sim$ 100 décimales)	107 itérations
10^{-1000} ($\sim$ 1000 décimales)	1073 itérations

Exemple 112. Erreur pour $(1,10)^{1/12}$

On pose $f(x) = x^{12} - 1,10$, $I = [1;1,10]$ et $\ell = (1,10)^{1/12}$. Comme $f'(x) = 12x^{11}$, si on pose de plus $m = 12$, on a $|f'(x)| \geqslant m$ pour $x \in I$. On obtient

$$\varepsilon_n = |\ell - a_n| \leqslant \frac{|a_n^{12} - 1,10|}{12}.$$

Par exemple $a_8 = 1.0079677973185432\ldots$ donc

$$|(1,10)^{1/12} - a_8| \leqslant \frac{|a_8^{12} - 1,10|}{12} = 6,92\ldots \cdot 10^{-6}.$$

2.5. Algorithme

Voici l'algorithme : c'est tout simplement la mise en œuvre de la suite récurrente (a_n).

Algorithme . secante.py

```
def secante(a,b,n) :
    for i in range(n) :
        a = a-f(a)*(b-a)/(f(b)-f(a))
    return a
```

Mini-exercices

1. À la main, calculer un encadrement à 0,1 près de $\sqrt{3}$. Idem avec $\sqrt[3]{2}$.
2. Calculer une approximation des solutions de l'équation $x^3 + 1 = 3x$.
3. Calculer une approximation de la solution de l'équation $(\cos x = 0)$ sur $[0,\pi]$. Idem avec $(\cos x = 2\sin x)$.

4. Étudier l'équation $(\exp(-x) = -\ln(x))$. Donner une approximation de la (ou des) solution(s) et une majoration de l'erreur correspondante.

3. La méthode de Newton

3.1. Méthode de Newton

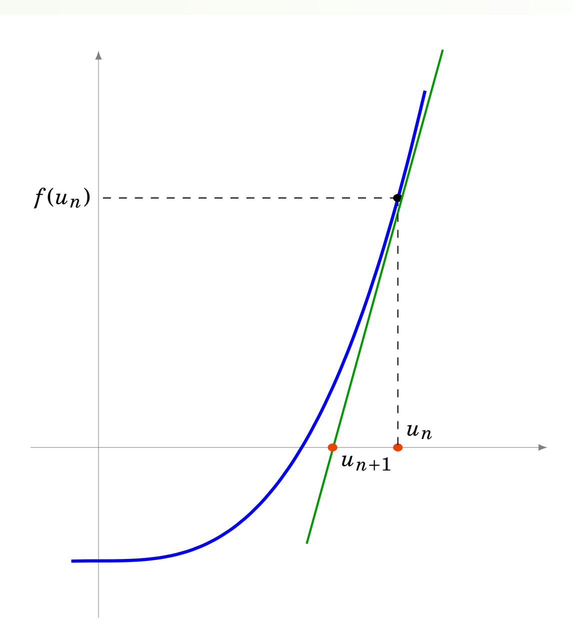
La méthode de Newton consiste à remplacer la sécante de la méthode précédente par la tangente. Elle est d'une redoutable efficacité.

Partons d'une fonction dérivable $f : [a,b] \to \mathbb{R}$ et d'un point $u_0 \in [a,b]$. On appelle $(u_1,0)$ l'intersection de la tangente au graphe de f en $(u_0, f(u_0))$ avec l'axe des abscisses. Si $u_1 \in [a,b]$ alors on recommence l'opération avec la tangente au point d'abscisse u_1. Ce processus conduit à la définition d'une suite récurrente :

$$u_0 \in [a,b] \qquad \text{et} \qquad u_{n+1} = u_n - \frac{f(u_n)}{f'(u_n)}.$$

Démonstration

En effet la tangente au point d'abscisse u_n a pour équation : $y = f'(u_n)(x - u_n) + f(u_n)$. Donc le point $(x,0)$ appartenant à la tangente (et à l'axe des abscisses) vérifie $0 = f'(u_n)(x-u_n)+f(u_n)$. D'où $x = u_n - \frac{f(u_n)}{f'(u_n)}$.



3.2. Résultats pour $\sqrt{10}$

Pour calculer $\sqrt{a}$, on pose $f(x) = x^2 - a$, avec $f'(x) = 2x$. La suite issue de la méthode de Newton est déterminée par $u_0 > 0$ et la relation de récurrence $u_{n+1} = u_n - \frac{u_n^2 - a}{2u_n}$. Suite qui pour cet exemple s'appelle ***suite de Héron*** et que l'on récrit souvent

$$\boxed{u_0 > 0 \quad \text{et} \quad u_{n+1} = \frac{1}{2}\left(u_n + \frac{a}{u_n}\right).}$$

Proposition 75

Cette suite (u_n) converge vers $\sqrt{a}$.

Pour le calcul de $\sqrt{10}$, on pose par exemple $u_0 = 4$, et on peut même commencer les calculs à la main :

$$\begin{aligned}
&u_0 = 4\\
&u_1 = \tfrac{1}{2}\left(u_0 + \tfrac{10}{u_0}\right) = \tfrac{1}{2}\left(4 + \tfrac{10}{4}\right) = \tfrac{13}{4} = 3,25\\
&u_2 = \tfrac{1}{2}\left(u_1 + \tfrac{10}{u_1}\right) = \tfrac{1}{2}\left(\tfrac{13}{4} + \tfrac{10}{\frac{13}{4}}\right) = \tfrac{329}{104} = 3,1634\ldots\\
&u_3 = \tfrac{1}{2}\left(u_2 + \tfrac{10}{u_2}\right) = \tfrac{216401}{68432} = 3,16227788\ldots\\
&u_4 = 3,162277660168387\ldots
\end{aligned}$$

Pour u_4 on obtient $\sqrt{10} = 3,1622776601683\ldots$ avec déjà 13 décimales exactes !
Voici la preuve de la convergence de la suite (u_n) vers $\sqrt{a}$.

Démonstration

$$u_0 > 0 \quad \text{et} \quad u_{n+1} = \frac{1}{2}\left(u_n + \frac{a}{u_n}\right).$$

1. Montrons que $u_n \geqslant \sqrt{a}$ pour $n \geqslant 1$.
   Tout d'abord
   $$u_{n+1}^2 - a = \frac{1}{4}\left(\frac{u_n^2 + a}{u_n}\right)^2 - a = \frac{1}{4u_n^2}(u_n^4 - 2au_n^2 + a^2) = \frac{1}{4}\frac{(u_n^2 - a)^2}{u_n^2}$$
   Donc $u_{n+1}^2 - a \geqslant 0$. Comme il est clair que pour tout $n \geqslant 0$, $u_n \geqslant 0$, on en déduit que pour tout $n \geqslant 0$, $u_{n+1} \geqslant \sqrt{a}$. (Notez que u_0 lui est quelconque.)
2. Montrons que $(u_n)_{n\geqslant 1}$ est une suite décroissante qui converge.
   Comme $\frac{u_{n+1}}{u_n} = \frac{1}{2}\left(1 + \frac{a}{u_n^2}\right)$, et que pour $n \geqslant 1$ on vient de voir que $u_n^2 \geqslant a$ (donc $\frac{a}{u_n^2} \leqslant 1$), alors $\frac{u_{n+1}}{u_n} \leqslant 1$, pour tout $n \leqslant 1$.
   Conséquence : la suite $(u_n)_{n\geqslant 1}$ est décroissante et minorée par 0 donc elle converge.
3. (u_n) converge vers $\sqrt{a}$.
   Notons ℓ la limite de (u_n). Alors $u_n \to \ell$ et $u_{n+1} \to \ell$. Lorsque $n \to +\infty$ dans la relation $u_{n+1} = \frac{1}{2}\left(u_n + \frac{a}{u_n}\right)$, on obtient $\ell = \frac{1}{2}\left(\ell + \frac{a}{\ell}\right)$. Ce qui conduit à la relation $\ell^2 = a$ et par positivité de la suite, $\ell = \sqrt{a}$.

3.3. Résultats numériques pour $(1,10)^{1/12}$

Pour calculer $(1,10)^{1/12}$, on pose $f(x) = x^{12} - a$ avec $a = 1,10$. On a $f'(x) = 12x^{11}$. On obtient $u_{n+1} = u_n - \frac{u_n^{12} - a}{12u_n^{11}}$. Ce que l'on reformule ainsi :

$$u_0 > 0 \quad \text{et} \quad u_{n+1} = \frac{1}{12}\left(11u_n + \frac{a}{u_n^{11}}\right).$$

Voici les résultats numériques pour $(1,10)^{1/12}$ en partant de $u_0 = 1$.

$$\begin{aligned}
&u_0 = 1\\
&u_1 = 1,0083333333333333\ldots\\
&u_2 = 1,0079748433368980\ldots\\
&u_3 = 1,0079741404315996\ldots\\
&u_4 = 1,0079741404289038\ldots
\end{aligned}$$

Toutes les décimales affichées pour u_4 sont exactes : $(1,10)^{1/12} = 1,0079741404289038\dots$

3.4. Calcul de l'erreur pour $\sqrt{10}$

Proposition 76

1. Soit k tel que $u_1 - \sqrt{a} \leqslant k$. Alors pour tout $n \geqslant 1$:
$$u_n - \sqrt{a} \leqslant 2\sqrt{a}\left(\frac{k}{2\sqrt{a}}\right)^{2^{n-1}}$$
2. Pour $a = 10$, $u_0 = 4$, on a :
$$u_n - \sqrt{10} \leqslant 8\left(\frac{1}{24}\right)^{2^{n-1}}$$

Admirez la puissance de la méthode de Newton : 11 itérations donnent déjà 1000 décimales exactes après la virgule. Cette rapidité de convergence se justifie grâce au calcul de l'erreur : la précision est multipliée par 2 à chaque étape, donc à chaque itération le nombre de décimales exactes double !

10^{-10} ($\sim$ 10 décimales)	4 itérations
10^{-100} ($\sim$ 100 décimales)	8 itérations
10^{-1000} ($\sim$ 1000 décimales)	11 itérations

Démonstration

1. Dans la preuve de la proposition 75, nous avons vu l'égalité :
$$u_{n+1}^2 - a = \frac{(u_n^2-a)^2}{4u_n^2} \quad \text{donc } (u_{n+1}-\sqrt{a})(u_{n+1}+\sqrt{a}) = \frac{(u_n-\sqrt{a})^2(u_n+\sqrt{a})^2}{4u_n^2}$$
Ainsi comme $u_n \geqslant \sqrt{a}$ pour $n \geqslant 1$:
$$u_{n+1}-\sqrt{a} = (u_n-\sqrt{a})^2 \times \frac{1}{u_{n+1}+\sqrt{a}} \times \frac{1}{4}\left(1+\frac{\sqrt{a}}{u_n}\right)^2 \leqslant (u_n-\sqrt{a})^2 \times \frac{1}{2\sqrt{a}} \times \frac{1}{4}\cdot(1+1)^2 = \frac{1}{2\sqrt{a}}(u_n-\sqrt{a})^2$$
Si k vérifie $u_1 - \sqrt{a} \leqslant k$, nous allons en déduire par récurrence, pour tout $n \geqslant 1$, la formule
$$u_n - \sqrt{a} \leqslant 2\sqrt{a}\left(\frac{k}{2\sqrt{a}}\right)^{2^{n-1}}$$
C'est vrai pour $n = 1$. Supposons la formule vraie au rang n, alors :
$$u_{n+1} - \sqrt{a} \leqslant \frac{1}{2\sqrt{a}}(u_n-\sqrt{a})^2 = \frac{1}{2\sqrt{a}}(2\sqrt{a})^2\left(\left(\frac{k}{2\sqrt{a}}\right)^{2^{n-1}}\right)^2 = 2\sqrt{a}\left(\frac{k}{2\sqrt{a}}\right)^{2^n}$$
La formule est donc vrai au rang suivant.
2. Pour $a = 10$ avec $u_0 = 4$ on a $u_1 = 3,25$. Comme $3 \leqslant \sqrt{10} \leqslant 4$ alors $u_1 - \sqrt{10} \leqslant u_1 - 3 \leqslant \frac{1}{4}$. On fixe donc $k = \frac{1}{4}$. Toujours par l'encadrement $3 \leqslant \sqrt{10} \leqslant 4$, la formule obtenue précédemment devient
$$u_n - \sqrt{a} \leqslant 2\cdot 4\left(\frac{\frac{1}{4}}{2\cdot 3}\right)^{2^{n-1}} = 8\left(\frac{1}{24}\right)^{2^{n-1}}.$$

3.5. Algorithme

Voici l'algorithme pour le calcul de $\sqrt{a}$. On précise en entrée le réel $a \geqslant 0$ dont on veut calculer la racine et le nombre n d'itérations.

Algorithme . newton.py

```
def racine_carree(a,n) :
    u=4                 # N'importe qu'elle valeur > 0
    for i in range(n) :
        u = 0.5*(u+a/u)
    return u
```

En utilisant le module `decimal` le calcul de u_n pour $n = 11$ donne 1000 décimales de $\sqrt{10}$:

3,
16227766016837933199889354443271853371955513932521
68268575048527925944386392382213442481083793002951
87347284152840055148548856030453880014690519596700
15390334492165717925994065915015347411333948412408
53169295770904715764610443692578790620378086099418
28371711548406328552999118596824564203326961604691
31433612894979189026652954361267617878135006138818
62785804636831349524780311437693346719738195131856
78403231241795402218308045872844614600253577579702
82864402902440797789603454398916334922265261206779
26516760310484366977937569261557205003698949094694
21850007358348844643882731109289109042348054235653
40390727401978654372593964172600130699000095578446
31096267906944183361301813028945417033158077316263
86395193793704654765220632063686587197822049312426
05345411160935697982813245229700079888352375958532
85792513629646865114976752171234595592380393756251
25369855194955325099947038843990336466165470647234
99979613234340302185705218783667634578951073298287
51579452157716521396263244383990184845609357626020

Mini-exercices

1. À la calculette, calculer les trois premières étapes pour une approximation de $\sqrt{3}$, sous forme de nombres rationnels. Idem avec $\sqrt[3]{2}$.
2. Implémenter la méthode de Newton, étant données une fonction f et sa dérivée f'.
3. Calculer une approximation des solutions de l'équation $x^3 + 1 = 3x$.
4. Soit $a > 0$. Comment calculer $\frac{1}{a}$ par une méthode de Newton ?
5. Calculer n de sorte que $u_n - \sqrt{10} \leqslant 10^{-\ell}$ (avec $u_0 = 4$, $u_{n+1} = \frac{1}{2}\left(u_n + \frac{a}{u_n}\right)$, $a = 10$).

Auteurs

Auteurs : Arnaud Bodin, Niels Borne, Laura Desideri
Dessins : Benjamin Boutin

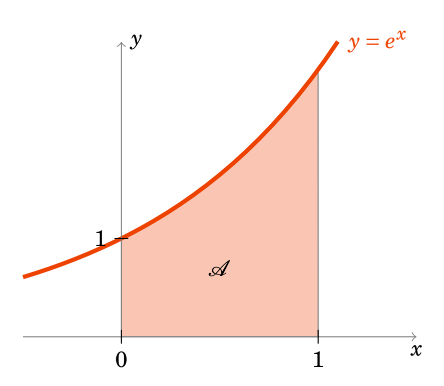


12 Intégrales

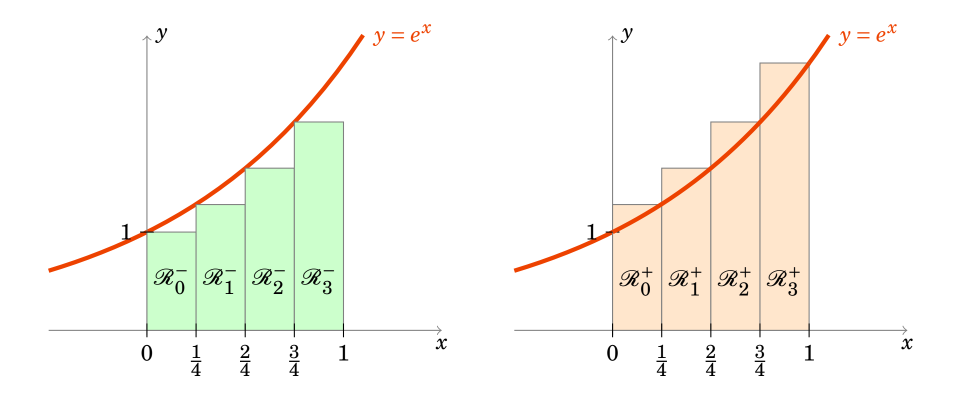
Vidéo ■ partie 1. L'intégrale de Riemann
Vidéo ■ partie 2. Propriétés
Vidéo ■ partie 3. Primitive
Vidéo ■ partie 4. Intégration par parties - Changement de variable
Vidéo ■ partie 5. Intégration des fractions rationnelles
Exercices ♦ Calculs d'intégrales

Motivation

Nous allons introduire l'intégrale à l'aide d'un exemple. Considérons la fonction exponentielle $f(x) = e^x$. On souhaite calculer l'aire $\mathscr{A}$ en-dessous du graphe de f et entre les droites d'équation $(x = 0)$, $(x = 1)$ et l'axe (Ox).



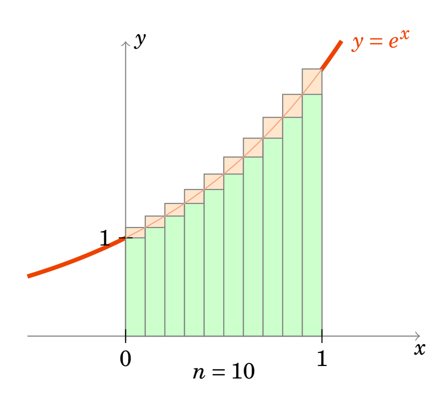
Nous approchons cette aire par des sommes d'aires des rectangles situés sous la courbe. Plus précisément, soit $n \geqslant 1$ un entier; découpons notre intervalle $[0,1]$ à l'aide de la subdivision $(0, \frac{1}{n}, \frac{2}{n}, \dots, \frac{i}{n}, \cdots, \frac{n-1}{n}, 1)$.
On considère les «rectangles inférieurs» $\mathscr{R}_i^-$, chacun ayant pour base l'intervalle $\left[\frac{i-1}{n}, \frac{i}{n}\right]$ et pour hauteur $f\left(\frac{i-1}{n}\right) = e^{(i-1)/n}$. L'entier i varie de 1 à n. L'aire de $\mathscr{R}_i^-$ est «base × hauteur» : $\left(\frac{i}{n} - \frac{i-1}{n}\right) \times e^{(i-1)/n} = \frac{1}{n} e^{\frac{i-1}{n}}$.



La somme des aires des $\mathscr{R}_i^-$ se calcule alors comme somme d'une suite géométrique :

$$\sum_{i=1}^{n} \frac{e^{\frac{i-1}{n}}}{n} = \frac{1}{n}\sum_{i=1}^{n}\left(e^{\frac{1}{n}}\right)^{i-1} = \frac{1}{n}\frac{1-\left(e^{\frac{1}{n}}\right)^n}{1-e^{\frac{1}{n}}} = \frac{\frac{1}{n}}{e^{\frac{1}{n}}-1}(e-1) \xrightarrow[n\to+\infty]{} e-1.$$

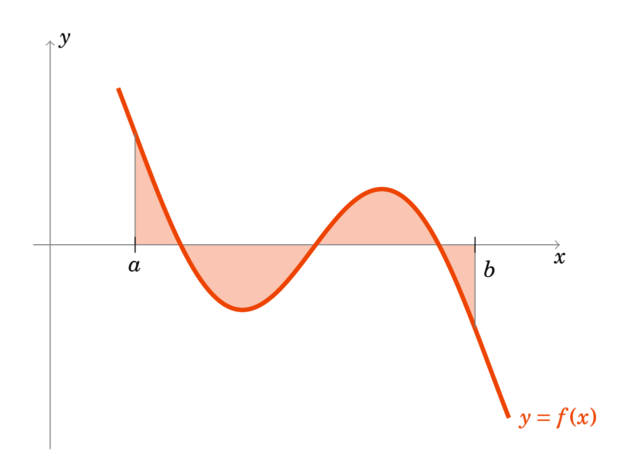
Pour la limite on a reconnu l'expression du type $\frac{e^x-1}{x} \xrightarrow[x\to 0]{} 1$ (avec ici $x = \frac{1}{n}$).
Soit maintenant les «rectangles supérieurs» $\mathscr{R}_i^+$, ayant la même base $\left[\frac{i-1}{n}, \frac{i}{n}\right]$ mais la hauteur $f\left(\frac{i}{n}\right) = e^{i/n}$. Un calcul similaire montre que $\sum_{i=1}^{n} \frac{e^{\frac{i}{n}}}{n} \to e-1$ lorsque $n \to +\infty$.
L'aire $\mathscr{A}$ de notre région est supérieure à la somme des aires des rectangles inférieurs ; et elle est inférieure à la somme des aires des rectangles supérieurs. Lorsque l'on considère des subdivisions de plus en plus petites (c'est-à-dire lorsque l'on fait tendre n vers $+\infty$) alors on obtient à la limite que l'aire $\mathscr{A}$ de notre région est encadrée par deux aires qui tendent vers $e-1$. Donc l'aire de notre région est $\mathscr{A} = e-1$.



Voici le plan de lecture conseillé pour ce chapitre : il est tout d'abord nécessaire de bien comprendre comment est définie l'intégrale et quelles sont ses principales propriétés (parties 1 et 2). Mais il est important d'arriver rapidement à savoir calculer des intégrales : à l'aide de primitives ou par les deux outils efficaces que sont l'intégration par parties et le changement de variable.
Dans un premier temps on peut lire les sections 1.1, 1.2 puis 2.1, 2.2, 2.3, avant de s'attarder longuement sur les parties 3, 4. Lors d'une seconde lecture, revenez sur la construction de l'intégrale et les preuves.
Dans ce chapitre on s'autorisera (abusivement) une confusion entre une fonction f et son expression $f(x)$. Par exemple on écrira « *une primitive de la fonction* $\sin x$ *est* $-\cos x$ » au lieu « *une primitive de la fonction* $x \mapsto \sin x$ *est* $x \mapsto -\cos x$ ».

1. L'intégrale de Riemann

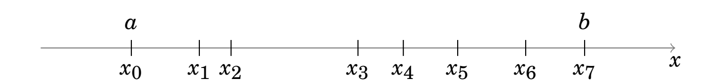
Nous allons reprendre la construction faite dans l'introduction pour une fonction f quelconque. Ce qui va remplacer les rectangles seront des ***fonctions en escalier***. Si la limite des aires en-dessous égale la limite des aires au-dessus on appelle cette limite commune ***l'intégrale*** de f que l'on note $\int_a^b f(x)\,dx$. Cependant il n'est pas toujours vrai que ces limites soit égales, l'intégrale n'est donc définie que pour les fonctions ***intégrables***. Heureusement nous verrons que si la fonction f est continue alors elle est intégrable.



1.1. Intégrale d'une fonction en escalier

Définition 62

Soit $[a,b]$ un intervalle fermé borné de $\mathbb{R}$ ($-\infty < a < b < +\infty$). On appelle une ***subdivision*** de $[a,b]$ une suite finie, strictement croissante, de nombres $\mathscr{S} = (x_0, x_1, \ldots, x_n)$ telle que $x_0 = a$ et $x_n = b$. Autrement dit $a = x_0 < x_1 < \ldots < x_n = b$.



Définition 63

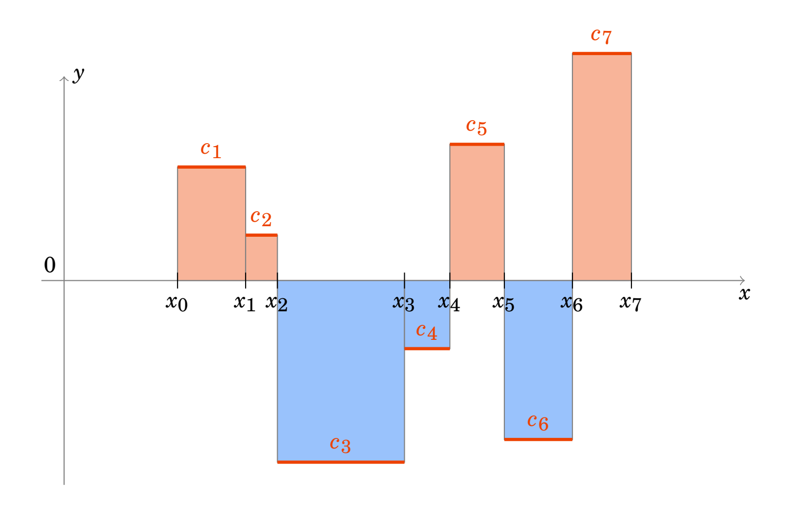
Une fonction $f : [a,b] \to \mathbb{R}$ est une ***fonction en escalier*** s'il existe une subdivision $(x_0, x_1, \ldots, x_n)$ et des nombres réels $c_1, \ldots, c_n$ tels que pour tout $i \in \{1, \ldots, n\}$ on ait

$$\forall x \in]x_{i-1}, x_i[\quad f(x) = c_i$$

Autrement dit f est une fonction constante sur chacun des sous-intervalles de la subdivision.

Remarque

La valeur de f aux points x_i de la subdivision n'est pas imposée. Elle peut être égale à celle de l'intervalle qui précède ou de celui qui suit, ou encore une autre valeur arbitraire. Cela n'a pas d'importance car l'aire ne changera pas.



Définition 64

Pour une fonction en escalier comme ci-dessus, son ***intégrale*** est le réel $\int_a^b f(x)\,dx$ défini par

$$\int_a^b f(x)\,dx = \sum_{i=1}^{n} c_i(x_i - x_{i-1})$$

Remarque

Notez que chaque terme $c_i(x_i - x_{i-1})$ est l'aire du rectangle compris entre les abscisses x_{i-1} et x_i et de hauteur c_i. Il faut juste prendre garde que l'on compte l'aire avec un signe «+» si $c_i > 0$ et un signe «−» si $c_i < 0$.
L'intégrale d'une fonction en escalier est l'aire de la partie située au-dessus de l'axe des abscisses (ici en rouge) moins l'aire de la partie située en-dessous (en bleu). L'intégrale d'une fonction en escalier est bien un nombre réel qui mesure l'aire algébrique (c'est-à-dire avec signe) entre la courbe de f et l'axe des abscisses.

1.2. Fonction intégrable

Rappelons qu'une fonction $f : [a,b] \to \mathbb{R}$ est ***bornée*** s'il existe $M \geqslant 0$ tel que :

$$\forall x \in [a,b] \quad -M \leqslant f(x) \leqslant M.$$

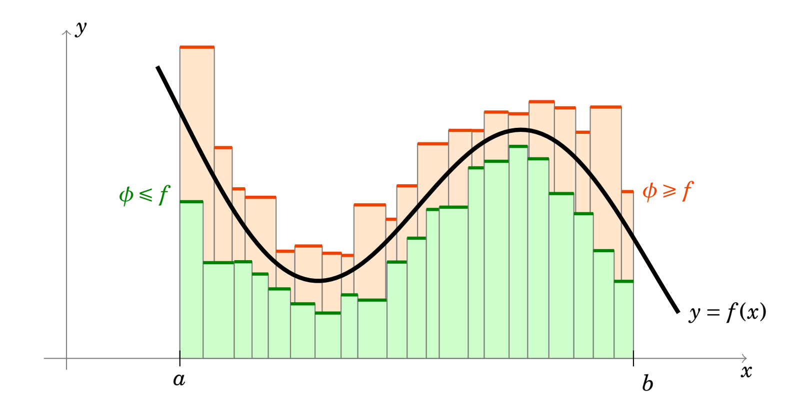
Rappelons aussi que si l'on a deux fonctions $f, g : [a,b] \to \mathbb{R}$, alors on note

$$f \leqslant g \qquad \Longleftrightarrow \qquad \forall x \in [a,b] \quad f(x) \leqslant g(x).$$

On suppose à présent que $f : [a,b] \to \mathbb{R}$ est une fonction bornée quelconque. On définit deux nombres réels :

$$I^-(f) = \sup\left\{ \int_a^b \phi(x)\,dx \mid \phi \text{ en escalier et } \phi \leqslant f \right\}$$

$$I^{+}(f) = \inf\left\{\int_a^b \phi(x)\,dx \mid \phi \text{ en escalier et } \phi \geqslant f\right\}$$



Pour $I^{-}(f)$ on prend toutes les fonctions en escalier (avec toutes les subdivisions possibles) qui restent inférieures à f. On prend l'aire la plus grande parmi toutes ces fonctions en escalier, comme on n'est pas sûr que ce maximum existe on prend la borne supérieure. Pour $I^{+}(f)$ c'est le même principe mais les fonctions en escalier sont supérieures à f et on cherche l'aire la plus petite possible.
Il est intuitif que l'on a :

Proposition 77

$I^{-}(f) \leqslant I^{+}(f)$.

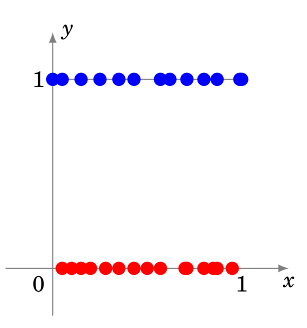
Les preuves sont reportées en fin de section.

Définition 65

Une fonction bornée $f : [a,b] \to \mathbb{R}$ est dite ***intégrable*** (***au sens de Riemann***) si $I^{-}(f) = I^{+}(f)$. On appelle alors ce nombre ***l'intégrale de Riemann*** de f sur $[a,b]$ et on le note $\int_a^b f(x)\,dx$.

Exemple 113

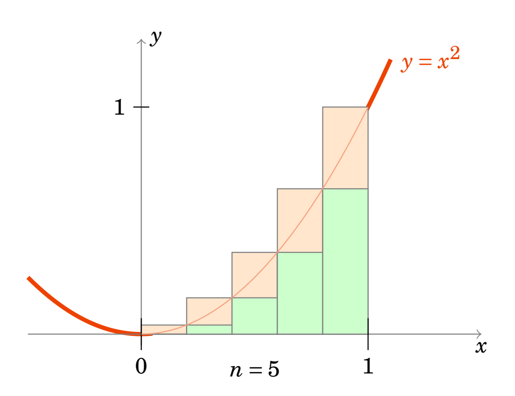
- Les fonctions en escalier sont intégrables ! En effet si f est une fonction en escalier alors la borne inférieure $I^{-}(f)$ et supérieure $I^{+}(f)$ sont atteintes avec la fonction $\phi = f$. Bien sûr l'intégrale $\int_a^b f(x)\,dx$ coïncide avec l'intégrale de la fonction en escalier définie lors du paragraphe 1.1.
- Nous verrons dans la section suivante que les fonctions continues et les fonctions monotones sont intégrables.
- Cependant toutes les fonctions ne sont pas intégrables. La fonction $f : [0,1] \to \mathbb{R}$ définie par $f(x) = 1$ si x est rationnel et $f(x) = 0$ sinon, n'est pas intégrable sur $[0,1]$. Convainquez-vous que si ϕ est une fonction en escalier avec $\phi \leqslant f$ alors $\phi \leqslant 0$ et que si $\phi \geqslant f$ alors $\phi \geqslant 1$. On en déduit que $I^{-}(f) = 0$ et $I^{+}(f) = 1$. Les bornes inférieure et supérieure ne coïncident pas, donc f n'est pas intégrable.



Il n'est pas si facile de calculer des exemples avec la définition. Nous allons vu l'exemple de la fonction exponentielle dans l'introduction où nous avions en fait montré que $\int_0^1 e^x\,dx = e-1$. Nous allons voir maintenant l'exemple de la fonction $f(x)=x^2$. Plus tard nous verrons que les primitives permettent de calculer simplement beaucoup d'intégrales.

Exemple 114

Soit $f:[0,1]\to\mathbb{R}$, $f(x)=x^2$. Montrons qu'elle est intégrable et calculons $\int_0^1 f(x)\,dx$.



Soit $n\geqslant 1$ et considérons la subdivision régulière de $[0,1]$ suivante $\mathscr{S}=\left(0,\frac{1}{n},\frac{2}{n},\ldots,\frac{i}{n},\ldots,\frac{n-1}{n},1\right)$. Sur l'intervalle $\left[\frac{i-1}{n},\frac{i}{n}\right]$ nous avons

$$\forall x\in\left[\tfrac{i-1}{n},\tfrac{i}{n}\right]\quad \left(\tfrac{i-1}{n}\right)^2\leqslant x^2\leqslant\left(\tfrac{i}{n}\right)^2.$$

Nous construisons une fonction en escalier ϕ^- en-dessous de f par $\phi^-(x)=\frac{(i-1)^2}{n^2}$ si $x\in\left[\frac{i-1}{n},\frac{i}{n}\right[$ (pour chaque $i=1,\ldots,n$) et $\phi^-(1)=1$. De même nous construisons une fonction en escalier ϕ^+ au-dessus de f définie par $\phi^+(x)=\frac{i^2}{n^2}$ si $x\in\left[\frac{i-1}{n},\frac{i}{n}\right[$ (pour chaque $i=1,\ldots,n$) et $\phi^+(1)=1$. ϕ^- et ϕ^+ sont des fonctions en escalier et l'on a $\phi^-\leqslant f\leqslant\phi^+$.
L'intégrale de la fonction en escalier ϕ^+ est par définition

$$\int_0^1\phi^+(x)\,dx=\sum_{i=1}^n\frac{i^2}{n^2}\left(\frac{i}{n}-\frac{i-1}{n}\right)=\sum_{i=1}^n\frac{i^2}{n^2}\frac{1}{n}=\frac{1}{n^3}\sum_{i=1}^n i^2.$$

On se souvient de la formule $\sum_{i=1}^n i^2=\frac{n(n+1)(2n+1)}{6}$, et donc

$$\int_0^1\phi^+(x)\,dx=\frac{n(n+1)(2n+1)}{6n^3}=\frac{(n+1)(2n+1)}{6n^2}.$$

De même pour la fonction ϕ^- :

$$\int_0^1\phi^-(x)\,dx=\sum_{i=1}^n\frac{(i-1)^2}{n^2}\frac{1}{n}=\frac{1}{n^3}\sum_{j=1}^{n-1}j^2=\frac{(n-1)n(2n-1)}{6n^3}=\frac{(n-1)(2n-1)}{6n^2}.$$

Maintenant $I^-(f)$ est la borne supérieure sur toutes les fonctions en escalier inférieures à f donc en particulier $I^-(f) \geqslant \int_0^1 \phi^-(x)\,dx$. De même $I^+(f) \leqslant \int_0^1 \phi^+(x)\,dx$. En résumé :

$$\frac{(n-1)(2n-1)}{6n^2} = \int_0^1 \phi^-(x)\,dx \leqslant I^-(f) \leqslant I^+(f) \leqslant \int_0^1 \phi^+(x)\,dx = \frac{(n+1)(2n+1)}{6n^2}.$$

Lorsque l'on fait tendre n vers $+\infty$ alors les deux extrémités tendent vers $\frac{1}{3}$. On en déduit que $I^-(f) = I^+(f) = \frac{1}{3}$. Ainsi f est intégrable et $\int_0^1 x^2\,dx = \frac{1}{3}$.

1.3. Premières propriétés

Proposition 78

1. Si $f : [a,b] \to \mathbb{R}$ est intégrable et si l'on change les valeurs de f en un nombre fini de points de $[a,b]$ alors la fonction f est toujours intégrable et la valeur de l'intégrale $\int_a^b f(x)\,dx$ ne change pas.
2. Si $f : [a,b] \to \mathbb{R}$ est intégrable alors la restriction de f à tout intervalle $[a',b'] \subset [a,b]$ est encore intégrable.

1.4. Les fonctions continues sont intégrables

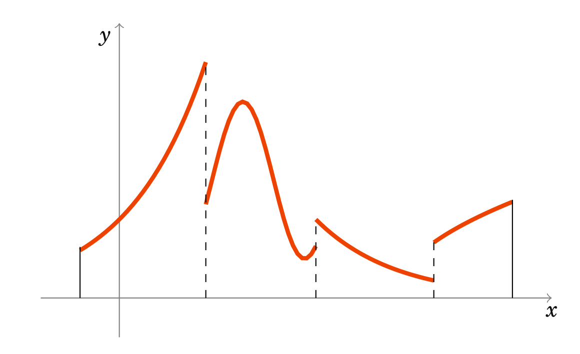
Voici le résultat théorique le plus important de ce chapitre.

Théorème 30

Si $f : [a,b] \to \mathbb{R}$ est continue alors f est intégrable.

La preuve sera vue plus loin mais l'idée est que les fonctions continues peuvent être approchées d'aussi près que l'on veut par des fonctions en escalier, tout en gardant un contrôle d'erreur uniforme sur l'intervalle.

Une fonction $f : [a,b] \to \mathbb{R}$ est dite ***continue par morceaux*** s'il existe un entier n et une subdivision $(x_0, \ldots, x_n)$ telle que $f_{|]x_{i-1},x_i[}$ soit continue, admette une limite finie à droite en x_{i-1} et une limite à gauche en x_i pour tout $i \in \{1, \ldots, n\}$.



Corollaire 17

Les fonctions continues par morceaux sont intégrables.

Voici un résultat qui prouve que l'on peut aussi intégrer des fonctions qui ne sont pas continues à condition que la fonction soit croissante (ou décroissante).

Théorème 31

Si $f : [a,b] \to \mathbb{R}$ est monotone alors f est intégrable.

1.5. Les preuves

Les preuves peuvent être sautées lors d'une première lecture. Les démonstrations demandent une bonne maîtrise des bornes sup et inf et donc des «epsilons». La proposition 77 se prouve en manipulant les «epsilons». Pour la preuve de la proposition 78 : on prouve d'abord les propriétés pour les fonctions en escalier et on en déduit qu'elles restent vraies pour les fonctions intégrables (cette technique sera développée en détails dans la partie suivante).
Le théorème 30 établit que les fonctions continues sont intégrables. Nous allons démontrer une version affaiblie de ce résultat. Rappelons que f est dite de ***classe*** $\mathscr{C}^1$ si f est continue, dérivable et f' est aussi continue.

Théorème 32. Théorème 30 faible

Si $f : [a,b] \to \mathbb{R}$ est de classe $\mathscr{C}^1$ alors f est intégrable.

Démonstration

Comme f est de classe $\mathscr{C}^1$ alors f' est une fonction continue sur l'intervalle fermé et borné $[a,b]$; f' est donc une fonction bornée : il existe $M \geqslant 0$ tel que pour tout $x \in [a,b]$ on ait $|f'(x)| \leqslant M$.
Nous allons utiliser l'inégalité des accroissements finis :

$$\forall x,y \in [a,b] \quad |f(x)-f(y)| \leqslant M|x-y|. \tag{$\star$}$$

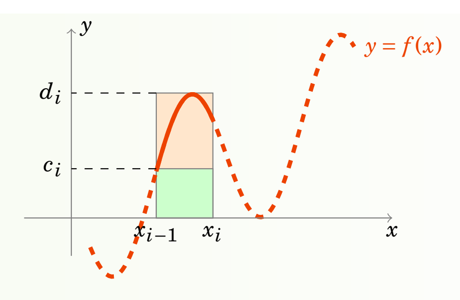
Soit $\varepsilon > 0$ et soit $(x_0,x_1,\dots,x_n)$ une subdivision de $[a,b]$ vérifiant pour tout $i = 1,\dots,n$:

$$0 < x_i - x_{i-1} \leqslant \varepsilon. \tag{$\star\star$}$$

Nous allons construire deux fonctions en escalier $\phi^-,\phi^+ : [a,b] \to \mathbb{R}$ définies de la façon suivante : pour chaque $i = 1,\dots,n$ et chaque $x \in [x_{i-1},x_i[$ on pose

$$c_i = \phi^-(x) = \inf_{t\in[x_{i-1},x_i[} f(t) \quad \text{et} \quad d_i = \phi^+(x) = \sup_{t\in[x_{i-1},x_i[} f(t)$$

et aussi $\phi^-(b) = \phi^+(b) = f(b)$. ϕ^- et ϕ^+ sont bien deux fonctions en escalier (elles sont constantes sur chaque intervalle $[x_{i-1},x_i[$).



De plus par construction on a bien $\phi^- \leqslant f \leqslant \phi^+$ et donc

$$\int_a^b \phi^-(x)\,dx \leqslant I^-(f) \leqslant I^+(f) \leqslant \int_a^b \phi^+(x)\,dx\,.$$

En utilisant la continuité de f sur l'intervalle $[x_{i-1},x_i]$, on déduit l'existence de $a_i,b_i \in [x_{i-1},x_i]$ tels que $f(a_i)=c_i$ et $f(b_i)=d_i$. Avec ($\star$) et ($\star\star$) on sait que $d_i - c_i = f(b_i)-f(a_i) \leqslant M|b_i - c_i| \leqslant M(x_i - x_{i-1}) \leqslant M\varepsilon$ (pour tout $i=1,\ldots,n$). Alors

$$\int_a^b \phi^+(x)\,dx - \int_a^b \phi^-(x)\,dx \leqslant \sum_{i=1}^n M\varepsilon(x_i - x_{i-1}) = M\varepsilon(b-a)$$

Ainsi $0 \leqslant I^+(f) - I^-(f) \leqslant M\varepsilon(b-a)$ et lorsque l'on fait tendre $\varepsilon \to 0$ on trouve $I^+(f) = I^-(f)$, ce qui prouve que f est intégrable.

La preuve du théorème 31 est du même style et nous l'omettons.

Mini-exercices

1. Soit $f : [1,4] \to \mathbb{R}$ définie par $f(x)=1$ si $x \in [1,2[$, $f(x)=3$ si $x \in [2,3[$ et $f(x)=-1$ si $x \in [3,4]$. Calculer $\int_1^2 f(x)\,dx$, $\int_1^3 f(x)\,dx$, $\int_1^4 f(x)\,dx$, $\int_1^{\frac{3}{2}} f(x)\,dx$, $\int_{\frac{3}{2}}^{\frac{7}{2}} f(x)\,dx$.
2. Montrer que $\int_0^1 x\,dx = 1$ (prendre une subdivision régulière et utiliser $\sum_{i=1}^n i = \frac{n(n+1)}{2}$).
3. Montrer que si f est une fonction intégrable et *paire* sur l'intervalle $[-a,a]$ alors $\int_{-a}^a f(x)\,dx = 2\int_0^a f(x)\,dx$ (on prendra une subdivision symétrique par rapport à l'origine).
4. Montrer que si f est une fonction intégrable et *impaire* sur l'intervalle $[-a,a]$ alors $\int_{-a}^a f(x)\,dx = 0$.
5. Montrer que tout fonction monotone est intégrable en s'inspirant de la preuve du théorème 32.

2. Propriétés de l'intégrale

Les trois principales propriétés de l'intégrale sont la relation de Chasles, la positivité et la linéarité.

2.1. Relation de Chasles

Proposition 79. Relation de Chasles

Soient $a < c < b$. Si f est intégrable sur $[a,c]$ et $[c,b]$, alors f est intégrable sur $[a,b]$. Et on a

$$\int_a^b f(x)\,dx = \int_a^c f(x)\,dx + \int_c^b f(x)\,dx$$

Pour s'autoriser des bornes sans se préoccuper de l'ordre on définit :

$$\int_a^a f(x)\,dx = 0 \qquad \text{et pour } a < b \quad \int_b^a f(x)\,dx = -\int_a^b f(x)\,dx.$$

Pour a, b, c quelconques la ***relation de Chasles*** devient alors

$$\boxed{\int_a^b f(x)\,dx = \int_a^c f(x)\,dx + \int_c^b f(x)\,dx}$$

2.2. Positivité de l'intégrale

Proposition 80. Positivité de l'intégrale

Soit $a \leqslant b$ deux réels et f et g deux fonctions intégrables sur $[a,b]$.

$$\boxed{\text{Si } f \leqslant g \quad \text{alors} \quad \int_a^b f(x)\,dx \leqslant \int_a^b g(x)\,dx}$$

En particulier l'intégrale d'une fonction positive est positive :

$$\boxed{\text{Si} \quad f \geqslant 0 \quad \text{alors} \quad \int_a^b f(x)\,dx \geqslant 0}$$

2.3. Linéarité de l'intégrale

Proposition 81

Soient f, g deux fonctions intégrables sur $[a,b]$.

1. $f+g$ est une fonction intégrable et $\int_a^b (f+g)(x)\,dx = \int_a^b f(x)\,dx + \int_a^b g(x)\,dx$.
2. Pour tout réel λ, λf est intégrable et on a $\int_a^b \lambda f(x)\,dx = \lambda \int_a^b f(x)\,dx$.
   Par ces deux premiers points nous avons la ***linéarité de l'intégrale*** : pour tous réels λ, μ
   $$\boxed{\int_a^b \big(\lambda f(x) + \mu g(x)\big)\,dx = \lambda \int_a^b f(x)\,dx + \mu \int_a^b g(x)\,dx}$$
3. $f \times g$ est une fonction intégrable sur $[a,b]$ mais en général $\int_a^b (fg)(x)\,dx \neq \big(\int_a^b f(x)\,dx\big)\big(\int_a^b g(x)\,dx\big)$.
4. $|f|$ est une fonction intégrable sur $[a,b]$ et
   $$\boxed{\left|\int_a^b f(x)\,dx\right| \leqslant \int_a^b \big|f(x)\big|\,dx}$$

Exemple 115

$$\int_0^1 \left(7x^2 - e^x\right) dx = 7\int_0^1 x^2\, dx \;-\; \int_0^1 e^x\, dx = 7\frac{1}{3} \;-\; (e-1) = \frac{10}{3} - e$$

Nous avons utilisé les calculs déjà vus : $\int_0^1 x^2\, dx = \frac{1}{3}$ et $\int_0^1 e^x\, dx = e-1$.

Exemple 116

Soit $I_n = \int_1^n \frac{\sin(nx)}{1+x^n}\, dx$. Montrons que $I_n \to 0$ lorsque $n \to +\infty$.

$$|I_n| = \left|\int_1^n \frac{\sin(nx)}{1+x^n}\, dx\right| \leqslant \int_1^n \frac{|\sin(nx)|}{1+x^n}\, dx \leqslant \int_1^n \frac{1}{1+x^n}\, dx \leqslant \int_1^n \frac{1}{x^n}\, dx$$

Il ne reste plus qu'à calculer cette dernière intégrale (en anticipant un peu sur la suite du chapitre) :

$$\int_1^n \frac{1}{x^n}\, dx = \int_1^n x^{-n}\, dx = \left[\frac{x^{-n+1}}{-n+1}\right]_1^n = \frac{n^{-n+1}}{-n+1} - \frac{1}{-n+1} \xrightarrow[n\to+\infty]{} 0$$

(car $n^{-n+1} \to 0$ et $\frac{1}{-n+1} \to 0$).

Remarque

Notez que même si $f \times g$ est intégrable on a en général $\int_a^b (fg)(x)\, dx \neq \left(\int_a^b f(x)\, dx\right)\left(\int_a^b g(x)\, dx\right)$. Par exemple, soit $f : [0,1] \to \mathbb{R}$ la fonction définie par $f(x) = 1$ si $x \in [0, \frac{1}{2}[$ et $f(x) = 0$ sinon. Soit $g : [0,1] \to \mathbb{R}$ la fonction définie par $g(x) = 1$ si $x \in [\frac{1}{2}, 1[$ et $g(x) = 0$ sinon. Alors $f(x) \times g(x) = 0$ pour tout $x \in [0,1]$ et donc $\int_0^1 f(x)g(x)\, dx = 0$ alors que $\int_0^1 f(x)\, dx = \frac{1}{2}$ et $\int_0^1 g(x)\, dx = \frac{1}{2}$.

2.4. Une preuve

Nous allons prouver la linéarité de l'intégrale : $\int \lambda f = \lambda \int f$ et $\int f + g = \int f + \int g$. L'idée est la suivante : il est facile de voir que pour des fonctions en escalier l'intégrale (qui est alors une somme finie) est linéaire. Comme les fonctions en escalier approchent autant qu'on le souhaite les fonctions intégrables alors cela implique la linéarité de l'intégrale.

Démonstration . Preuve de $\int \lambda f = \lambda \int f$

Soit $f : [a,b] \to \mathbb{R}$ une fonction intégrable et $\lambda \in \mathbb{R}$. Soit $\varepsilon > 0$.
Il existe ϕ^- et ϕ^+ deux fonctions en escalier approchant suffisamment f, avec $\phi^- \leqslant f \leqslant \phi^+$:

$$\int_a^b f(x)\, dx \;-\varepsilon \;\leqslant \int_a^b \phi^-(x)\, dx \qquad \text{et} \qquad \int_a^b \phi^+(x)\, dx \;\leqslant \int_a^b f(x)\, dx \;+\varepsilon \tag{†}$$

Quitte à rajouter des points, on peut supposer que la subdivision $(x_0, x_1, \ldots, x_n)$ de $[a,b]$ est suffisamment fine pour que ϕ^- et ϕ^+ soient toutes les deux constantes sur les intervalles $]x_{i-1}, x_i[$; on note c_i^- et c_i^+ leurs valeurs respectives.
Dans un premier temps on suppose $\lambda \geqslant 0$. Alors $\lambda\phi^-$ et $\lambda\phi^+$ sont encore des fonctions en escalier vérifiant $\lambda\phi^- \leqslant \lambda f \leqslant \lambda\phi^+$. De plus

$$\int_a^b \lambda\phi^-(x)\, dx = \sum_{i=1}^n \lambda c_i^-(x_i - x_{i-1}) = \lambda \sum_{i=1}^n c_i^-(x_i - x_{i-1}) = \lambda \int_a^b \phi^-(x)\, dx$$

De même pour ϕ^+. Ainsi

$$\lambda\int_a^b \phi^-(x)\,dx \leqslant I^-(\lambda f) \leqslant I^+(\lambda f) \leqslant \lambda\int_a^b \phi^+(x)\,dx$$

En utilisant les deux inégalités (†) on obtient

$$\lambda\int_a^b f(x)\,dx - \lambda\varepsilon \leqslant I^-(\lambda f) \leqslant I^+(\lambda f) \leqslant \lambda\int_a^b f(x)\,dx + \lambda\varepsilon$$

Lorsque l'on fait tendre $\varepsilon \to 0$ cela prouve que $I^-(\lambda f) = I^+(\lambda f)$, donc λf est intégrable et $\int_a^b \lambda f(x)\,dx = \lambda\int_a^b f(x)\,dx$. Si $\lambda \leqslant 0$ on a $\lambda\phi^+ \leqslant \lambda f \leqslant \lambda\phi^-$ et le raisonnement est similaire.

Démonstration . Preuve de $\int f + g = \int f + \int g$

Soit $\varepsilon > 0$. Soient $f, g : [a,b] \to \mathbb{R}$ deux fonctions intégrables. On définit deux fonctions en escalier ϕ^+, ϕ^- pour f et deux fonctions en escalier ψ^+, ψ^- pour g vérifiant des inégalités similaires à (†) de la preuve au-dessus. On fixe une subdivision suffisamment fine pour toutes les fonctions $\phi^\pm, \psi^\pm$. On note $c_i^\pm, d_i^\pm$ les constantes respectives sur l'intervalle $]x_{i-1}, x_i[$. Les fonctions $\phi^- + \psi^-$ et $\phi^+ + \psi^+$ sont en escalier et vérifient $\phi^- + \psi^- \leqslant f + g \leqslant \phi^+ + \psi^+$. Nous avons aussi que

$$\int_a^b (\phi^- + \psi^-)(x)\,dx = \sum_{i=1}^n (c_i^- + d_i^-)(x_i - x_{i-1}) = \int_a^b \phi^-(x)\,dx + \int_a^b \psi^-(x)\,dx$$

De même pour $\phi^+ + \psi^+$. Ainsi

$$\int_a^b \phi^-(x)\,dx + \int_a^b \psi^-(x)\,dx \leqslant I^-(f+g) \leqslant I^+(f+g) \leqslant \int_a^b \phi^+(x)\,dx + \int_a^b \psi^+(x)\,dx$$

Les conditions du type (†) impliquent alors

$$\int_a^b f(x)\,dx + \int_a^b g(x)\,dx - 2\varepsilon \leqslant I^-(f+g) \leqslant I^+(f+g) \leqslant \int_a^b f(x)\,dx + \int_a^b g(x)\,dx + 2\varepsilon$$

Lorsque $\varepsilon \to 0$ on déduit $I^-(f+g) = I^+(f+g)$, donc $f+g$ est intégrable et $\int_a^b \big(f(x)+g(x)\big)\,dx = \int_a^b f(x)\,dx + \int_a^b g(x)\,dx$.

Mini-exercices

1. En admettant que $\int_0^1 x^n\,dx = \frac{1}{n+1}$. Calculer l'intégrale $\int_0^1 P(x)\,dx$ où $P(x) = a_n x^n + \cdots + a_1 x + a_0$. Trouver un polynôme $P(x)$ non nul de degré 2 dont l'intégrale est nulle : $\int_0^1 P(x)\,dx = 0$.
2. A-t-on $\int_a^b f(x)^2\,dx = \left(\int_a^b f(x)\,dx\right)^2$; $\int_a^b \sqrt{f(x)}\,dx = \sqrt{\int_a^b f(x)\,dx}$; $\int_a^b |f(x)|\,dx = \left|\int_a^b f(x)\,dx\right|$; $\int |f(x)+g(x)|\,dx = \left|\int_a^b f(x)\,dx\right| + \left|\int_a^b g(x)\,dx\right|$?
3. Peut-on trouver $a < b$ tels que $\int_a^b x\,dx = -1$; $\int_a^b x\,dx = 0$; $\int_a^b x\,dx = +1$? Mêmes questions avec $\int_a^b x^2\,dx$.
4. Montrer que $0 \leqslant \int_1^2 \sin^2 x\,dx \leqslant 1$ et $\left|\int_a^b \cos^3 x\,dx\right| \leqslant |b-a|$.

3. Primitive d'une fonction

3.1. Définition

Définition 66

Soit $f : I \to \mathbb{R}$ une fonction définie sur un intervalle I quelconque. On dit que $F : I \to \mathbb{R}$ est une ***primitive*** de f sur I si F est une fonction dérivable sur I vérifiant $F'(x) = f(x)$ pour tout $x \in I$.

Trouver une primitive est donc l'opération inverse de calculer la fonction dérivée.

Exemple 117

1. Soit $I = \mathbb{R}$ et $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$. Alors $F : \mathbb{R} \to \mathbb{R}$ définie par $F(x) = \frac{x^3}{3}$ est une primitive de f. La fonction définie par $F(x) = \frac{x^3}{3} + 1$ est aussi une primitive de f.
2. Soit $I = [0, +\infty[$ et $g : I \to \mathbb{R}$ définie par $g(x) = \sqrt{x}$. Alors $G : I \to \mathbb{R}$ définie par $G(x) = \frac{2}{3}x^{\frac{3}{2}}$ est une primitive de g sur I. Pour tout $c \in \mathbb{R}$, la fonction $G + c$ est aussi une primitive de g.

Nous allons voir que trouver une primitive permet de les trouver toutes.

Proposition 82

Soit $f : I \to \mathbb{R}$ une fonction et soit $F : I \to \mathbb{R}$ une primitive de f. Toute primitive de f s'écrit $G = F + c$ où $c \in \mathbb{R}$.

Démonstration

Notons tout d'abord que si l'on note G la fonction définie par $G(x) = F(x) + c$ alors $G'(x) = F'(x)$ mais comme $F'(x) = f(x)$ alors $G'(x) = f(x)$ et G est bien une primitive de f.
Pour la réciproque supposons que G soit une primitive quelconque de f. Alors $(G - F)'(x) = G'(x) - F'(x) = f(x) - f(x) = 0$, ainsi la fonction $G - F$ a une dérivée nulle sur un intervalle, c'est donc une fonction constante ! Il existe donc $c \in \mathbb{R}$ tel que $(G - F)(x) = c$. Autrement dit $G(x) = F(x) + c$ (pour tout $x \in I$).

Notations On notera une primitive de f par $\int f(t)\,dt$ ou $\int f(x)\,dx$ ou $\int f(u)\,du$ (les lettres $t, x, u, \dots$ sont des lettres dites *muettes*, c'est-à-dire interchangeables). On peut même noter une primitive simplement par $\int f$.
La proposition 82 nous dit que si F est une primitive de f alors il existe un réel c, tel que $F = \int f(t)\,dt + c$.
Attention : $\int f(t)\,dt$ désigne une fonction de I dans $\mathbb{R}$ alors que l'intégrale $\int_a^b f(t)\,dt$ désigne un nombre réel. Plus précisément nous verrons que si F est une primitive de f alors $\int_a^b f(t)\,dt = F(b) - F(a)$.

Par dérivation on prouve facilement le résultat suivant :

Proposition 83

Soient F une primitive de f et G une primitive de g. Alors $F + G$ est une primitive de $f + g$. Et si $\lambda \in \mathbb{R}$ alors λF est une primitive de λf.

Une autre formulation est de dire que pour tous réels λ, μ on a

$$\int \big(\lambda f(t) + \mu g(t)\big)\,dt = \lambda \int f(t)\,dt + \mu \int g(t)\,dt$$

3.2. Primitives des fonctions usuelles

$\int e^x \, dx = e^x + c \quad$ sur $\mathbb{R}$
$\int \cos x \, dx = \sin x + c \quad$ sur $\mathbb{R}$
$\int \sin x \, dx = -\cos x + c \quad$ sur $\mathbb{R}$
$\int x^n \, dx = \frac{x^{n+1}}{n+1} + c \quad (n \in \mathbb{N}) \quad$ sur $\mathbb{R}$
$\int x^\alpha \, dx = \frac{x^{\alpha+1}}{\alpha+1} + c \quad (\alpha \in \mathbb{R} \setminus \{-1\})$ sur $]0, +\infty[$
$\int \frac{1}{x} \, dx = \ln \lvert x \rvert + c \quad$ sur $]0, +\infty[$ ou $]-\infty, 0[$

$\int \operatorname{sh} x \, dx = \operatorname{ch} x + c, \int \operatorname{ch} x \, dx = \operatorname{sh} x + c \quad$ sur $\mathbb{R}$
$\int \frac{dx}{1+x^2} = \arctan x + c \quad$ sur $\mathbb{R}$
$\int \frac{dx}{\sqrt{1-x^2}} = \begin{cases} \arcsin x + c \\ \frac{\pi}{2} - \arccos x + c \end{cases}$ sur $]-1, 1[$
$\int \frac{dx}{\sqrt{x^2+1}} = \begin{cases} \operatorname{argsh} x + c \\ \ln\left(x + \sqrt{x^2+1}\right) + c \end{cases}$ sur $\mathbb{R}$
$\int \frac{dx}{\sqrt{x^2-1}} = \begin{cases} \operatorname{argch} x + c \\ \ln\left(x + \sqrt{x^2-1}\right) + c \end{cases}$ sur $x \in]1, +\infty[$

Remarque

Ces primitives sont à connaître par cœur.

1. Voici comment lire ce tableau. Si f est la fonction définie sur $\mathbb{R}$ par $f(x) = x^n$ alors la fonction $: x \mapsto \frac{x^{n+1}}{n+1}$ est une primitive de f sur $\mathbb{R}$. Les primitives de f sont les fonctions définies par $x \mapsto \frac{x^{n+1}}{n+1} + c$ (pour c une constante réelles quelconque). Et on écrit $\int x^n \, dx = \frac{x^{n+1}}{n+1} + c$, où $c \in \mathbb{R}$.
2. Souvenez vous que la variable sous le symbole intégrale est une variable muette. On peut aussi bien écrire $\int t^n \, dt = \frac{x^{n+1}}{n+1} + c$.
3. La constante est définie pour un intervalle. Si l'on a deux intervalles, il y a deux constantes qui peuvent être différentes. Par exemple pour $\int \frac{1}{x} \, dx$ nous avons deux domaines de validité : $I_1 =]0, +\infty[$ et $I_2 =]-\infty, 0[$. Donc $\int \frac{1}{x} \, dx = \ln x + c_1$ si $x > 0$ et $\int \frac{1}{x} \, dx = \ln \lvert x \rvert + c_2 = \ln(-x) + c_2$ si $x < 0$.
4. On peut trouver des primitives aux allures très différentes par exemple $x \mapsto \arcsin x$ et $x \mapsto \frac{\pi}{2} - \arccos x$ sont deux primitives de la même fonction $x \mapsto \frac{1}{\sqrt{1-x^2}}$. Mais bien sûr on sait que $\arcsin x + \arccos x = \frac{\pi}{2}$, donc les primitives diffèrent bien d'une constante !

3.3. Relation primitive-intégrale

Théorème 33

Soit $f : [a,b] \to \mathbb{R}$ une fonction continue. La fonction $F : I \to \mathbb{R}$ définie par

$$F(x) = \int_a^x f(t)\,dt$$

est une primitive de f, c'est-à-dire F est dérivable et $F'(x) = f(x)$.
Par conséquent pour une primitive F quelconque de f :

$$\int_a^b f(t)\,dt = F(b) - F(a)$$

Notation. On note $\left[F(x)\right]_a^b = F(b) - F(a)$.

Exemple 118

Nous allons pouvoir calculer plein d'intégrales. Recalculons d'abord les intégrales déjà rencontrées.

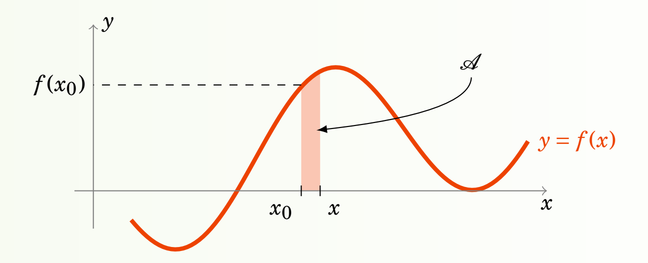
1. Pour $f(x) = e^x$ une primitive est $F(x) = e^x$ donc
$$\int_0^1 e^x\,dx = \left[e^x\right]_0^1 = e^1 - e^0 = e - 1.$$
2. Pour $g(x) = x^2$ une primitive est $G(x) = \frac{x^3}{3}$ donc
$$\int_0^1 x^2\,dx = \left[\tfrac{x^3}{3}\right]_0^1 = \tfrac{1}{3}.$$
3. $\int_a^x \cos t\,dt = \left[\sin t\right]_{t=a}^{t=x} = \sin x - \sin a$ est une primitive de $\cos x$.
4. Si f est impaire alors ses primitives sont paires (le montrer). En déduire que $\int_{-a}^a f(t)\,dt = 0$.

Remarque

1. $F(x) = \int_a^x f(t)\,dt$ est même ***l'unique primitive de f qui s'annule en a***.
2. En particulier si F est une fonction de classe $\mathscr{C}^1$ alors $\int_a^b F'(t)\,dt = F(b) - F(a)$.
3. On évitera la notation $\int_a^x f(x)\,dx$ où la variable x est présente à la fois aux bornes et à l'intérieur de l'intégrale. Mieux vaut utiliser la notation $\int_a^x f(t)\,dt$ ou $\int_a^x f(u)\,du$ pour éviter toute confusion.
4. Une fonction intégrable n'admet pas forcément une primitive. Considérer par exemple $f : [0,1] \to \mathbb{R}$ définie par $f(x) = 0$ si $x \in [0, \frac{1}{2}[$ et $f(x) = 1$ si $x \in [\frac{1}{2}, 1]$. f est intégrable sur $[0,1]$ mais elle n'admet pas de primitive sur $[0,1]$. En effet par l'absurde si F était une primitive de F, par exemple la primitive qui vérifie $F(0) = 0$. Alors $F(x) = 0$ pour $x \in [0, \frac{1}{2}[$ et $F(x) = x - \frac{1}{2}$ pour $x \in [\frac{1}{2}, 1]$. Mais alors nous obtenons une contradiction car F n'est pas dérivable en $\frac{1}{2}$ alors que par définition une primitive doit être dérivable.

Démonstration

Essayons de visualiser tout d'abord pourquoi la fonction F est dérivable et $F'(x) = f(x)$.



Fixons $x_0 \in [a,b]$. Par la relation de Chasles nous savons :

$$F(x) - F(x_0) = \int_a^x f(t)\,dt - \int_a^{x_0} f(t)\,dt = \int_{x_0}^a f(t)\,dt + \int_a^x f(t)\,dt = \int_{x_0}^x f(t)\,dt$$

Donc le taux d'accroissement

$$\frac{F(x)-F(x_0)}{x-x_0} = \frac{1}{x-x_0}\int_{x_0}^x f(t)\,dt = \frac{\mathscr{A}}{x-x_0}$$

où $\mathscr{A}$ est l'aire hachurée (en rouge). Mais cette aire hachurée est presque un rectangle, si x est suffisamment proche de x_0, donc l'aire $\mathscr{A}$ vaut environ $(x-x_0)\times f(x_0)$ lorsque $x \to x_0$ le taux d'accroissement tend donc vers $f(x_0)$. Autrement dit $F'(x_0) = f(x_0)$.

Passons à la preuve rigoureuse. Comme $f(x_0)$ est une constante alors $\int_{x_0}^x f(x_0)\,dt = (x-x_0)f(x_0)$, donc

$$\frac{F(x)-F(x_0)}{x-x_0} - f(x_0) = \frac{1}{x-x_0}\int_{x_0}^x f(t)\,dt - \frac{1}{x-x_0}\int_{x_0}^x f(x_0)\,dt = \frac{1}{x-x_0}\int_{x_0}^x \big(f(t)-f(x_0)\big)\,dt$$

Fixons $\varepsilon > 0$. Puisque f est continue en x_0, il existe $\delta > 0$ tel que $(|t-x_0| < \delta \implies |f(t)-f(x_0)| < \varepsilon)$. Donc :

$$\left|\frac{F(x)-F(x_0)}{x-x_0} - f(x_0)\right| = \left|\frac{1}{x-x_0}\int_{x_0}^x \big(f(t)-f(x_0)\big)\,dt\right| \leqslant \frac{1}{|x-x_0|}\left|\int_{x_0}^x \big|f(t)-f(x_0)\big|\,dt\right| \leqslant \frac{1}{|x-x_0|}\left|\int_{x_0}^x \varepsilon\,dt\right| = \varepsilon$$

Ce qui prouve que F est dérivable en x_0 et $F'(x_0) = f(x_0)$.

Maintenant on sait que F est une primitive de f, F est même la primitive qui s'annule en a car $F(a) = \int_a^a f(t)\,dt = 0$. Si G est une autre primitive on sait $F = G + c$. Ainsi

$$G(b) - G(a) = F(b) + c - \big(F(a) + c\big) = F(b) - F(a) = F(b) = \int_a^b f(t)\,dt.$$

3.4. Sommes de Riemann

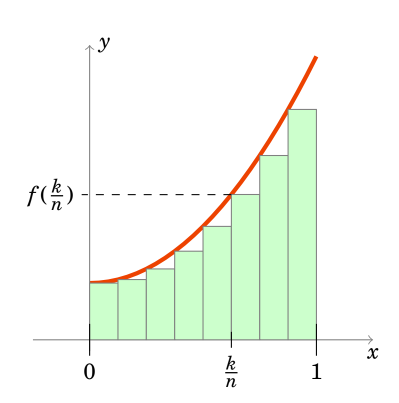
L'intégrale est définie à partir de limites de sommes. Mais maintenant que nous savons calculer des intégrales sans utiliser ces sommes on peut faire le cheminement inverse : calculer des limites de sommes à partir d'intégrales.

Théorème 34

$$S_n = \frac{b-a}{n}\sum_{k=1}^{n} f\left(a+k\frac{b-a}{n}\right) \xrightarrow[n\to+\infty]{} \int_a^b f(x)\,dx$$

La somme S_n s'appelle la ***somme de Riemann*** associée à l'intégrale et correspond à une subdivision régulière de l'intervalle $[a,b]$ en n petits intervalles. La hauteur de chaque rectangle étant évaluée à son extrémité droite.
Le cas le plus utile est le cas où $a=0$, $b=1$ alors $\frac{b-a}{n}=\frac{1}{n}$ et $f\left(a+k\frac{b-a}{n}\right)=f\left(\frac{k}{n}\right)$ et ainsi

$$S_n = \frac{1}{n}\sum_{k=1}^{n} f\left(\frac{k}{n}\right) \xrightarrow[n\to+\infty]{} \int_0^1 f(x)\,dx$$



Exemple 119

Calculer la limite de la somme $S_n=\sum_{k=1}^{n}\frac{1}{n+k}$.
On a $S_1=\frac{1}{2}$, $S_2=\frac{1}{3}+\frac{1}{4}$, $S_3=\frac{1}{4}+\frac{1}{5}+\frac{1}{6}$, $S_4=\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}$,...
La somme S_n s'écrit aussi $S_n=\frac{1}{n}\sum_{k=1}^{n}\frac{1}{1+\frac{k}{n}}$. En posant $f(x)=\frac{1}{1+x}$, $a=0$ et $b=1$, on reconnaît que S_n est une somme de Riemann. Donc

$$S_n=\frac{1}{n}\sum_{k=1}^{n}\frac{1}{1+\frac{k}{n}}=\frac{1}{n}\sum_{k=1}^{n}f\left(\frac{k}{n}\right)\xrightarrow[n\to+\infty]{}\int_a^b f(x)\,dx=\int_0^1\frac{1}{1+x}\,dx=\left[\ln|1+x|\right]_0^1=\ln 2-\ln 1=\ln 2.$$

Ainsi $S_n\to\ln 2$ (lorsque $n\to+\infty$).

Mini-exercices

1. Trouver les primitives des fonctions : x^3-x^7, $\cos x+\exp x$, $\sin(2x)$, $1+\sqrt{x}+x$, $\frac{1}{\sqrt{x}}$, $\sqrt[3]{x}$, $\frac{1}{x+1}$.
2. Trouver les primitives des fonctions : $\mathrm{ch}(x)-\mathrm{sh}(\frac{x}{2})$, $\frac{1}{1+4x^2}$, $\frac{1}{\sqrt{1+x^2}}-\frac{1}{\sqrt{1-x^2}}$.
3. Trouver une primitive de x^2e^x sous la forme $(ax^2+bx+c)e^x$.
4. Trouver toutes les primitives de $x\mapsto\frac{1}{x^2}$ (préciser les intervalles et les constantes).
5. Calculer les intégrales $\int_0^1 x^n\,dx$, $\int_0^{\frac{\pi}{4}}\frac{dx}{1+x^2}$, $\int_1^e\frac{1-x}{x^2}\,dx$, $\int_0^{\frac{1}{2}}\frac{dx}{x^2-1}$.
6. Calculer la limite (lorsque $n\to+\infty$) de la somme $S_n=\sum_{k=0}^{n}\frac{e^{k/n}}{n}$. Idem avec $S'_n=$

$\sum_{k=0}^{n} \frac{n}{(n+k)^2}$.

4. Intégration par parties – Changement de variable

Pour trouver une primitive d'une fonction f on peut avoir la chance de reconnaître que f est la dérivée d'une fonction bien connue. C'est malheureusement très rarement le cas, et on ne connaît pas les primitives de la plupart des fonctions. Cependant nous allons voir deux techniques qui permettent des calculer des intégrales et des primitives : l'intégration par parties et le changement de variable.

4.1. Intégration par parties

Théorème 35

Soient u et v deux fonctions de classe $\mathscr{C}^1$ sur un intervalle $[a,b]$.

$$\int_a^b u(x)v'(x)\,dx = \big[uv\big]_a^b - \int_a^b u'(x)v(x)\,dx$$

Notation. Le crochet $\big[F\big]_a^b$ est par définition $\big[F\big]_a^b = F(b)-F(a)$. Donc $\big[uv\big]_a^b = u(b)v(b)-u(a)v(a)$. Si l'on omet les bornes alors $\big[F\big]$ désigne la fonction $F+c$ où c est une constante quelconque.
La formule d'intégration par parties pour les primitives est la même mais sans les bornes :

$$\int u(x)v'(x)\,dx = \big[uv\big] - \int u'(x)v(x)\,dx.$$

La preuve est très simple :

Démonstration

On a $(uv)' = u'v+uv'$. Donc $\int_a^b (u'v+uv') = \int_a^b (uv)' = \big[uv\big]_a^b$. D'où $\int_a^b uv' = \big[uv\big]_a^b - \int_a^b u'v$.

L'utilisation de l'intégration par parties repose sur l'idée suivante : on ne sait pas calculer directement l'intégrale d'une fonction f s'écrivant comme un produit $f(x) = u(x)v'(x)$ mais si l'on sait calculer l'intégrale de $g(x) = u'(x)v(x)$ (que l'on espère plus simple) alors par la formule d'intégration par parties on aura l'intégrale de f.

Exemple 120

1. Calcul de $\int_0^1 xe^x\,dx$. On pose $u(x) = x$ et $v'(x) = e^x$. Nous aurons besoin de savoir que $u'(x) = 1$ et qu'une primitive de v' est simplement $v(x) = e^x$. La formule d'intégration par parties donne :

$$\begin{aligned}
\int_0^1 xe^x\,dx &= \int_0^1 u(x)v'(x)\,dx \\
&= \big[u(x)v(x)\big]_0^1 - \int_0^1 u'(x)v(x)\,dx \\
&= \big[xe^x\big]_0^1 \;-\; \int_0^1 1\cdot e^x\,dx \\
&= \left(1\cdot e^1 - 0\cdot e^0\right) - \big[e^x\big]_0^1 \\
&= e-(e^1-e^0) \\
&= 1
\end{aligned}$$

2. Calcul de $\int_1^e x\ln x\,dx$.

On pose cette fois $u = \ln x$ et $v' = x$. Ainsi $u' = \frac{1}{x}$ et $v = \frac{x^2}{2}$. Alors

$$\int_1^e \ln x \cdot x\,dx = \int_1^e uv' = [uv]_1^e - \int_1^e u'v = \left[\ln x \cdot \tfrac{x^2}{2}\right]_1^e - \int_1^e \tfrac{1}{x}\tfrac{x^2}{2}\,dx$$
$$= \left(\ln e \tfrac{e^2}{2} - \ln 1 \tfrac{1^2}{2}\right) - \tfrac{1}{2}\int_1^e x\,dx = \tfrac{e^2}{2} - \frac{1}{2}\left[\tfrac{x^2}{2}\right]_1^e = \tfrac{e^2}{2} - \tfrac{e^2}{4} + \tfrac{1}{4} = \tfrac{e^2+1}{4}$$

3. Calcul de $\int \arcsin x\,dx$.
   Pour déterminer une primitive de $\arcsin x$ nous faisons artificiellement apparaître un produit en écrivant $\arcsin x = 1 \cdot \arcsin x$ pour appliquer la formule d'intégration par parties. On pose $u = \arcsin x$, $v' = 1$ (et donc $u' = \frac{1}{\sqrt{1-x^2}}$ et $v = x$) alors

$$\int 1 \cdot \arcsin x\,dx = \left[x \arcsin x\right] - \int \frac{x}{\sqrt{1-x^2}}\,dx = \left[x \arcsin x\right] - \left[-\sqrt{1-x^2}\right] = x \arcsin x + \sqrt{1-x^2} + c$$

4. Calcul de $\int x^2 e^x\,dx$. On pose $u = x^2$ et $v' = e^x$ pour obtenir :

$$\int x^2 e^x\,dx = \left[x^2 e^x\right] - 2\int x e^x\,dx$$

   On refait une deuxième intégration par parties pour calculer

$$\int x e^x\,dx = \left[x e^x\right] - \int e^x\,dx = (x-1)e^x + c$$

   D'où

$$\int x^2 e^x\,dx = (x^2 - 2x + 2)e^x + c.$$

Exemple 121

Nous allons étudier les intégrales définies par $I_n = \displaystyle\int_0^1 \frac{\sin(\pi x)}{x+n}\,dx$, pour tout entier $n > 0$.

1. Montrer que $0 \leqslant I_{n+1} \leqslant I_n$.
   Pour $0 \leqslant x \leqslant 1$, on a $0 < x+n \leqslant x+n+1$ et $\sin(\pi x) \geqslant 0$, donc $0 \leqslant \frac{\sin(\pi x)}{x+n+1} \leqslant \frac{\sin(\pi x)}{x+n}$. D'où $0 \leqslant I_{n+1} \leqslant I_n$ par la positivité de l'intégrale.
2. Montrer que $I_n \leqslant \ln \frac{n+1}{n}$. En déduire $\lim_{n\to+\infty} I_n$.
   De $0 \leqslant \sin(\pi x) \leqslant 1$, on a $\frac{\sin(\pi x)}{x+n} \leqslant \frac{1}{x+n}$. D'où $0 \leqslant I_n \leqslant \int_0^1 \frac{1}{x+n}\,dx = \left[\ln(x+n)\right]_0^1 = \ln \frac{n+1}{n} \to 0$.
3. Calculer $\lim_{n\to+\infty} nI_n$.
   Nous allons faire une intégration par parties avec $u = \frac{1}{x+n}$ et $v' = \sin(\pi x)$ (et donc $u' = -\frac{1}{(x+n)^2}$ et $v = -\frac{1}{\pi}\cos(\pi x)$) :

$$nI_n = n\int_0^1 \frac{1}{x+n}\sin(\pi x)\,dx = -\frac{n}{\pi}\left[\frac{1}{x+n}\cos(\pi x)\right]_0^1 - \frac{n}{\pi}\int_0^1 \frac{1}{(x+n)^2}\cos(\pi x)\,dx = \frac{n}{\pi(n+1)} + \frac{1}{\pi} - \frac{n}{\pi}J_n$$

   Il nous reste à évaluer $J_n = \int_0^1 \frac{\cos(\pi x)}{(x+n)^2}\,dx$.

$$\left|\frac{n}{\pi}J_n\right| \leqslant \frac{n}{\pi}\int_0^1 \frac{|\cos(\pi x)|}{(x+n)^2}\,dx \leqslant \frac{n}{\pi}\int_0^1 \frac{1}{(x+n)^2}\,dx = \frac{n}{\pi}\left[-\frac{1}{x+n}\right]_0^1 = \frac{n}{\pi}\left(-\frac{1}{1+n} + \frac{1}{n}\right) = \frac{1}{\pi}\frac{1}{n+1} \to 0.$$

   Donc $\lim_{n\to+\infty} nI_n = \lim_{n\to+\infty} \frac{n}{\pi(n+1)} + \frac{1}{\pi} - \frac{n}{\pi}J_n = \frac{2}{\pi}$.

4.2. Changement de variable

Théorème 36

Soit f une fonction définie sur un intervalle I et $\varphi : J \to I$ une bijection de classe $\mathscr{C}^1$. Pour tout $a, b \in J$

$$\boxed{\int_{\varphi(a)}^{\varphi(b)} f(x)\,dx = \int_a^b f\big(\varphi(t)\big)\cdot\varphi'(t)\,dt}$$

Si F est une primitive de f alors $F\circ\varphi$ est une primitive de $\big(f\circ\varphi\big)\cdot\varphi'$.

Voici un moyen simple de s'en souvenir. En effet si l'on note $x = \varphi(t)$ alors par dérivation on obtient $\frac{dx}{dt} = \varphi'(t)$ donc $dx = \varphi'(t)\,dt$. D'où la substitution $\int_{\varphi(a)}^{\varphi(b)} f(x)\,dx = \int_a^b f(\varphi(t))\,\varphi'(t)\,dt$.

Démonstration

Comme F est une primitive de f alors $F'(x) = f(x)$ et par la formule de la dérivation de la composition $F\circ\varphi$ on a

$$(F\circ\varphi)'(t) = F'(\varphi(t))\varphi'(t) = f(\varphi(t))\varphi'(t).$$

Donc $F\circ\varphi$ est une primitive de $f(\varphi(t))\varphi'(t)$.

Pour les intégrales : $\displaystyle\int_a^b f(\varphi(t))\varphi'(t)\,dt = \big[F\circ\varphi\big]_a^b = F\big(\varphi(b)\big) - F\big(\varphi(a)\big) = \big[F\big]_{\varphi(a)}^{\varphi(b)} = \int_{\varphi(a)}^{\varphi(b)} f(x)\,dx.$

Remarque

Comme φ est une bijection de J sur $\varphi(J)$, sa réciproque φ^{-1} existe et est dérivable sauf quand φ s'annule. Si φ ne s'annule pas, on peut écrire $t = \varphi^{-1}(x)$ et faire un changement de variable en sens inverse.

Exemple 122

Calculons la primitive $F = \int \tan t\,dt$.

$$F = \int \tan t\,dt = \int \frac{\sin t}{\cos t}\,dt\,.$$

On reconnaît ici une forme $\frac{u'}{u}$ (avec $u = \cos t$ et $u' = -\sin t$) dont une primitive est $\ln|u|$. Donc $F = \int -\frac{u'}{u} = -\big[\ln|u|\big] = -\ln|u| + c = -\ln|\cos t| + c$.

Nous allons reformuler tout cela en terme de changement de variable. Notons $\varphi(t) = \cos t$ alors $\varphi'(t) = -\sin t$, donc

$$F = \int -\frac{\varphi'(t)}{\varphi(t)}\,dt$$

Si f désigne la fonction définie par $f(x) = \frac{1}{x}$, qui est bijective tant que $x \neq 0$; alors $F = -\int \varphi'(t) f(\varphi(t))\,dt$. En posant $x = \varphi(t)$ et donc $dx = \varphi'(t)dt$, on reconnaît la formule du changement de variable, par conséquent

$$F\circ\varphi^{-1} = -\int f(x)\,dx = -\int \frac{1}{x}\,dx = -\ln|x| + c\,.$$

Comme $x = \varphi(t) = \cos t$, on retrouve bien $F(t) = -\ln|\cos t| + c$.

Remarque : pour que l'intégrale soit bien définie il faut que $\tan t$ soit définie, donc $t \not\equiv \frac{\pi}{2} \mod \pi$. La restriction d'une primitive à un intervalle $]-\frac{\pi}{2}+k\pi, \frac{\pi}{2}+k\pi[$ est donc de la forme $-\ln|\cos t|+c$. Mais la constante c peut être différente sur un intervalle différent.

Exemple 123

Calcul de $\int_0^{1/2} \frac{x}{(1-x^2)^{3/2}}\,dx$.
Soit le changement de variable $u = \varphi(x) = 1-x^2$. Alors $du = \varphi'(x)\,dx = -2x\,dx$. Pour $x = 0$ on a $u = \varphi(0) = 1$ et pour $x = \frac{1}{2}$ on a $u = \varphi(\frac{1}{2}) = \frac{3}{4}$. Comme $\varphi'(x) = -2x$, φ est une bijection de $[0, \frac{1}{2}]$ sur $[0, \frac{3}{4}]$. Alors

$$\int_0^{1/2} \frac{x\,dx}{(1-x^2)^{3/2}} = \int_1^{3/4} \frac{\frac{-du}{2}}{u^{3/2}} = -\frac{1}{2}\int_1^{3/4} u^{-3/2}\,du = -\frac{1}{2}\big[-2u^{-1/2}\big]_1^{3/4} = \big[\frac{1}{\sqrt{u}}\big]_1^{3/4} = \frac{1}{\sqrt{\frac{3}{4}}} - 1 = \frac{2}{\sqrt{3}} - 1.$$

Exemple 124

Calcul de $\int_0^{1/2} \frac{1}{(1-x^2)^{3/2}}\,dx$.
On effectue le changement de variable $x = \varphi(t) = \sin t$ et $dx = \cos t\,dt$. De plus $t = \arcsin x$ donc pour $x = 0$ on a $t = \arcsin(0) = 0$ et pour $x = \frac{1}{2}$ on a $t = \arcsin(\frac{1}{2}) = \frac{\pi}{6}$. Comme φ est une bijection de $[0, \frac{\pi}{6}]$ sur $[0, \frac{1}{2}]$,

$$\int_0^{1/2} \frac{dx}{(1-x^2)^{3/2}} = \int_0^{\pi/6} \frac{\cos t\,dt}{(1-\sin^2 t)^{3/2}} = \int_0^{\pi/6} \frac{\cos t\,dt}{(\cos^2 t)^{3/2}} = \int_0^{\pi/6} \frac{\cos t}{\cos^3 t}\,dt = \int_0^{\pi/6} \frac{1}{\cos^2 t}\,dt = \big[\tan t\big]_0^{\pi/6} = \frac{1}{\sqrt{3}}.$$

Exemple 125

Calcul de $\int \frac{1}{(1+x^2)^{3/2}}\,dx$.
Soit le changement de variable $x = \tan t$ donc $t = \arctan x$ et $dx = \frac{dt}{\cos^2 t}$. Donc

$$\begin{aligned} F = \int \frac{1}{(1+x^2)^{3/2}}\,dx &= \int \frac{1}{(1+\tan^2 t)^{3/2}} \frac{dt}{\cos^2 t} \\ &= \int (\cos^2 t)^{3/2} \frac{dt}{\cos^2 t} \qquad \text{car } 1+\tan^2 t = \frac{1}{\cos^2 t} \\ &= \int \cos t\,dt = \big[\sin t\big] = \sin t + c = \sin(\arctan x) + c \end{aligned}$$

Donc

$$\int \frac{1}{(1+x^2)^{3/2}}\,dx = \sin(\arctan x) + c.$$

En manipulant un peu les fonctions on trouverait que la primitive s'écrit aussi $F(x) = \frac{x}{\sqrt{1+x^2}} + c$.

Mini-exercices

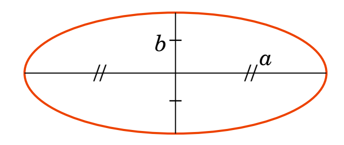
1. Calculer les intégrales à l'aide d'intégrations par parties : $\int_0^{\pi/2} t \sin t\,dt$, $\int_0^{\pi/2} t^2 \sin t\,dt$, puis par récurrence $\int_0^{\pi/2} t^n \sin t\,dt$.
2. Déterminer les primitives à l'aide d'intégrations par parties : $\int t \operatorname{sh} t\,dt$, $\int t^2 \operatorname{sh} t\,dt$, puis par récurrence $\int t^n \operatorname{sh} t\,dt$.

3. Calculer les intégrales à l'aide de changements de variable : $\int_0^a \sqrt{a^2-t^2}\,dt$; $\int_{-\pi}^{\pi} \sqrt{1+\cos t}\,dt$ (pour ce dernier poser deux changements de variables : $u = \cos t$, puis $v = 1-u$).
4. Déterminer les primitives suivantes à l'aide de changements de variable : $\int \operatorname{th} t\,dt$ où $\operatorname{th} t = \frac{\operatorname{sh} t}{\operatorname{ch} t}$, $\int e^{\sqrt{t}}\,dt$.

5. Intégration des fractions rationnelles

Nous savons intégrer beaucoup de fonctions simples. Par exemple toutes les fonctions polynomiales : si $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ alors $\int f(x)\,dx = a_0x + a_1\frac{x^2}{2} + a_2\frac{x^3}{3} + \cdots + a_n\frac{x^{n+1}}{n+1} + c$.

Il faut être conscient cependant que beaucoup de fonctions ne s'intègrent pas à l'aide de fonctions simples. Par exemple si $f(t) = \sqrt{a^2\cos^2 t + b^2\sin^2 t}$ alors l'intégrale $\int_0^{2\pi} f(t)\,dt$ ne peut pas s'exprimer comme somme, produit, inverse ou composition de fonctions que vous connaissez. En fait cette intégrale vaut la longueur d'une ellipse d'équation paramétrique $(a\cos t, b\sin t)$; il n'y a donc pas de formule pour le périmètre d'une ellipse (sauf si $a = b$ auquel cas l'ellipse est un cercle !).



Mais de façon remarquable, il y a toute une famille de fonctions que l'on saura intégrer : les fractions rationnelles.

5.1. Trois situations de base

On souhaite d'abord intégrer les fractions rationnelles $f(x) = \frac{\alpha x+\beta}{ax^2+bx+c}$ avec $\alpha,\beta,a,b,c \in \mathbb{R}$, $a \neq 0$ et $(\alpha,\beta) \neq (0,0)$.

Premier cas. Le dénominateur ax^2+bx+c possède deux racines réelles distinctes $x_1, x_2 \in \mathbb{R}$.
Alors $f(x)$ s'écrit aussi $f(x) = \frac{\alpha x+\beta}{a(x-x_1)(x-x_2)}$ et il existe de nombres $A, B \in \mathbb{R}$ tels que $f(x) = \frac{A}{x-x_1} + \frac{B}{x-x_2}$.
On a donc

$$\int f(x)\,dx = A\ln|x-x_1| + B\ln|x-x_2| + c$$

sur chacun des intervalles $]-\infty, x_1[$, $]x_1, x_2[$, $]x_2, +\infty[$ (si $x_1 < x_2$).

Deuxième cas. Le dénominateur ax^2+bx+c possède une racine double $x_0 \in \mathbb{R}$.
Alors $f(x) = \frac{\alpha x+\beta}{a(x-x_0)^2}$ et il existe des nombres $A, B \in \mathbb{R}$ tels que $f(x) = \frac{A}{(x-x_0)^2} + \frac{B}{x-x_0}$. On a alors

$$\int f(x)\,dx = -\frac{A}{x-x_0} + B\ln|x-x_0| + c$$

sur chacun des intervalles $]-\infty, x_0[$, $]x_0, +\infty[$.

Troisième cas. Le dénominateur ax^2+bx+c ne possède pas de racine réelle. Voyons comment faire sur un exemple.

Exemple 126

Soit $f(x) = \frac{x+1}{2x^2+x+1}$. Dans un premier temps on fait apparaître une fraction du type $\frac{u'}{u}$ (que l'on sait intégrer en $\ln|u|$).

$$f(x) = \frac{(4x+1)\frac{1}{4} - \frac{1}{4} + 1}{2x^2+x+1} = \frac{1}{4}\cdot\frac{4x+1}{2x^2+x+1} + \frac{3}{4}\cdot\frac{1}{2x^2+x+1}$$

On peut intégrer la fraction $\frac{4x+1}{2x^2+x+1}$:

$$\int \frac{4x+1}{2x^2+x+1}\,dx = \int \frac{u'(x)}{u(x)}\,dx = \ln\left|2x^2+x+1\right| + c$$

Occupons nous de l'autre partie $\frac{1}{2x^2+x+1}$, nous allons l'écrire sous la forme $\frac{1}{u^2+1}$ (dont une primitive est $\arctan u$).

$$\frac{1}{2x^2+x+1} = \frac{1}{2(x+\frac14)^2-\frac18+1} = \frac{1}{2(x+\frac14)^2+\frac78} = \frac{8}{7}\cdot\frac{1}{\frac{8}{7}2(x+\frac14)^2+1} = \frac{8}{7}\cdot\frac{1}{\left(\frac{4}{\sqrt7}(x+\frac14)\right)^2+1}$$

On pose le changement de variable $u = \frac{4}{\sqrt7}(x+\frac14)$ (et donc $du = \frac{4}{\sqrt7}dx$) pour trouver

$$\int \frac{dx}{2x^2+x+1} = \int \frac{8}{7}\frac{dx}{\left(\frac{4}{\sqrt7}(x+\frac14)\right)^2+1} = \frac{8}{7}\int \frac{du}{u^2+1}\cdot\frac{\sqrt7}{4} = \frac{2}{\sqrt7}\arctan u + c = \frac{2}{\sqrt7}\arctan\left(\frac{4}{\sqrt7}(x+\frac14)\right)+c\,.$$

Finalement :

$$\int f(x)\,dx = \frac14\ln\left(2x^2+x+1\right) + \frac{3}{2\sqrt7}\arctan\left(\frac{4}{\sqrt7}(x+\frac14)\right)+c$$

5.2. Intégration des éléments simples

Soit $\frac{P(x)}{Q(x)}$ une fraction rationnelle, où $P(x),Q(x)$ sont des polynômes à coefficients réels. Alors la fraction $\frac{P(x)}{Q(x)}$ s'écrit comme somme d'un polynôme $E(x) \in \mathbb{R}[x]$ (la partie entière) et d'éléments simples d'une des formes suivantes :

$$\frac{\gamma}{(x-x_0)^k} \quad \text{ou} \quad \frac{\alpha x+\beta}{(ax^2+bx+c)^k} \text{ avec } b^2-4ac<0$$

où $\alpha,\beta,\gamma,a,b,c \in \mathbb{R}$ et $k \in \mathbb{N}\setminus\{0\}$.

1. On sait intégrer le polynôme $E(x)$.
2. Intégration de l'élément simple $\frac{\gamma}{(x-x_0)^k}$.
   (a) Si $k=1$ alors $\int \frac{\gamma\,dx}{x-x_0} = \gamma\ln|x-x_0|+c$ (sur $]-\infty,x_0[$ ou $]x_0,+\infty[$).
   (b) Si $k \geqslant 2$ alors $\int \frac{\gamma\,dx}{(x-x_0)^k} = \gamma\int(x-x_0)^{-k}\,dx = \frac{\gamma}{-k+1}(x-x_0)^{-k+1}+c$ (sur $]-\infty,x_0[$ ou $]x_0,+\infty[$).
3. Intégration de l'élément simple $\frac{\alpha x+\beta}{(ax^2+bx+c)^k}$. On écrit cette fraction sous la forme

$$\frac{\alpha x+\beta}{(ax^2+bx+c)^k} = \gamma\frac{2ax+b}{(ax^2+bx+c)^k} + \delta\frac{1}{(ax^2+bx+c)^k}$$

   (a) $\int \frac{2ax+b}{(ax^2+bx+c)^k}\,dx = \int \frac{u'(x)}{u(x)^k}\,dx = \frac{1}{-k+1}u(x)^{-k+1}+c = \frac{1}{-k+1}(ax^2+bx+c)^{-k+1}+c$.
   (b) Si $k=1$, calcul de $\int \frac{1}{ax^2+bx+c}\,dx$. Par un changement de variable $u = px+q$ on se ramène à calculer une primitive du type $\int \frac{du}{u^2+1} = \arctan u + c$.
   (c) Si $k \geqslant 2$, calcul de $\int \frac{1}{(ax^2+bx+c)^k}\,dx$. On effectue le changement de variable $u = px+q$ pour se ramener au calcul de $I_k = \int \frac{du}{(u^2+1)^k}$. Une intégration par parties permet de passer de I_k à I_{k-1}.
   Par exemple calculons I_2. Partant de $I_1 = \int \frac{du}{u^2+1}$ on pose $f = \frac{1}{u^2+1}$ et $g'=1$. La formule d'intégration par parties $\int fg' = [fg] - \int f'g$ donne (avec $f' = -\frac{2u}{(u^2+1)^2}$ et $g=u$)

$$\begin{aligned} I_1 &= \int \frac{du}{u^2+1} = \left[\frac{u}{u^2+1}\right] + \int \frac{2u^2\,du}{(u^2+1)^2} = \left[\frac{u}{u^2+1}\right] + 2\int \frac{u^2+1-1}{(u^2+1)^2}du \\ &= \left[\frac{u}{u^2+1}\right] + 2\int \frac{du}{u^2+1} - 2\int \frac{du}{(u^2+1)^2} = \left[\frac{u}{u^2+1}\right] + 2I_1 - 2I_2 \end{aligned}$$

On en déduit $I_2 = \frac{1}{2}I_1 + \frac{1}{2}\frac{u}{u^2+1} + c$. Mais comme $I_1 = \arctan u$ alors

$$I_2 = \int \frac{du}{(u^2+1)^2} = \frac{1}{2}\arctan u + \frac{1}{2}\frac{u}{u^2+1} + c.$$

5.3. Intégration des fonctions trigonométriques

On peut aussi calculer les primitives de la forme $\int P(\cos x, \sin x)\,dx$ ou $\int \frac{P(\cos x,\sin x)}{Q(\cos x,\sin x)}\,dx$ quand P et Q sont des polynômes, en se ramenant à intégrer une fraction rationnelle.
Il existe deux méthodes :

- les règles de Bioche sont assez efficaces mais ne fonctionnent pas toujours ;
- le changement de variable $t = \tan \frac{x}{2}$ fonctionne tout le temps mais conduit à davantage de calculs.

Les règles de Bioche. On note $\omega(x) = f(x)\,dx$. On a alors $\omega(-x) = f(-x)\,d(-x) = -f(-x)\,dx$ et $\omega(\pi - x) = f(\pi - x)\,d(\pi - x) = -f(\pi - x)\,dx$.

- Si $\omega(-x) = \omega(x)$ alors on effectue le changement de variable $u = \cos x$.
- Si $\omega(\pi - x) = \omega(x)$ alors on effectue le changement de variable $u = \sin x$.
- Si $\omega(\pi + x) = \omega(x)$ alors on effectue le changement de variable $u = \tan x$.

Exemple 127

Calcul de la primitive $\int \frac{\cos x\,dx}{2-\cos^2 x}$
On note $\omega(x) = \frac{\cos x\,dx}{2-\cos^2 x}$. Comme $\omega(\pi - x) = \frac{\cos(\pi-x)\,d(\pi-x)}{2-\cos^2(\pi-x)} = \frac{(-\cos x)(-dx)}{2-\cos^2 x} = \omega(x)$ alors le changement de variable qui convient est $u = \sin x$ pour lequel $du = \cos x\,dx$. Ainsi :

$$\int \frac{\cos x\,dx}{2-\cos^2 x} = \int \frac{\cos x\,dx}{2-(1-\sin^2 x)} = \int \frac{du}{1+u^2} = \big[\arctan u\big] = \arctan(\sin x) + c\,.$$

Le changement de variable $t = \tan \frac{x}{2}$.
Les formules de la «tangente de l'arc moitié» permettent d'exprimer sinus, cosinus et tangente en fonction de $\tan \frac{x}{2}$.

Avec $\quad t = \tan \frac{x}{2} \quad$ on a $\quad \cos x = \frac{1-t^2}{1+t^2} \quad \sin x = \frac{2t}{1+t^2} \quad \tan x = \frac{2t}{1-t^2} \quad$ et $\quad dx = \frac{2\,dt}{1+t^2}$.

Exemple 128

Calcul de l'intégrale $\int_{-\pi/2}^{0} \frac{dx}{1-\sin x}$.
Le changement de variable $t = \tan \frac{x}{2}$ définit une bijection de $[-\frac{\pi}{2}, 0]$ vers $[-1, 0]$ (pour $x = -\frac{\pi}{2}$, $t = -1$ et pour $x = 0$, $t = 0$). De plus on a $\sin x = \frac{2t}{1+t^2}$ et $dx = \frac{2\,dt}{1+t^2}$.

$$\int_{-\frac{\pi}{2}}^{0} \frac{dx}{1-\sin x} = \int_{-1}^{0} \frac{\frac{2\,dt}{1+t^2}}{1-\frac{2t}{1+t^2}} = 2\int_{-1}^{0} \frac{dt}{1+t^2-2t} = 2\int_{-1}^{0} \frac{dt}{(1-t)^2} = 2\left[\frac{1}{1-t}\right]_{-1}^{0} = 2\big(1-\frac{1}{2}\big) = 1$$

Mini-exercices

1. Calculer les primitives $\int \frac{4x+5}{x^2+x-2}\,dx$, $\int \frac{6-x}{x^2-4x+4}\,dx$, $\int \frac{2x-4}{(x-2)^2+1}\,dx$, $\int \frac{1}{(x-2)^2+1}\,dx$.
2. Calculer les primitives $I_k = \int \frac{dx}{(x-1)^k}$ pour tout $k \geqslant 1$. Idem avec $J_k = \int \frac{x\,dx}{(x^2+1)^k}$.
3. Calculer les intégrales suivantes : $\int_0^1 \frac{dx}{x^2+x+1}$, $\int_0^1 \frac{x\,dx}{x^2+x+1}$, $\int_0^1 \frac{x\,dx}{(x^2+x+1)^2}$, $\int_0^1 \frac{dx}{(x^2+x+1)^2}$.
4. Calculer les intégrales suivantes : $\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \sin^2 x \cos^3 x\,dx$, $\int_0^{\frac{\pi}{2}} \cos^4 x\,dx$, $\int_0^{2\pi} \frac{dx}{2+\sin x}$.

Auteurs

Rédaction : Arnaud Bodin

Basé sur des cours de Guoting Chen et Marc Bourdon

Relecture : Pascal Romon

Dessins : Benjamin Boutin

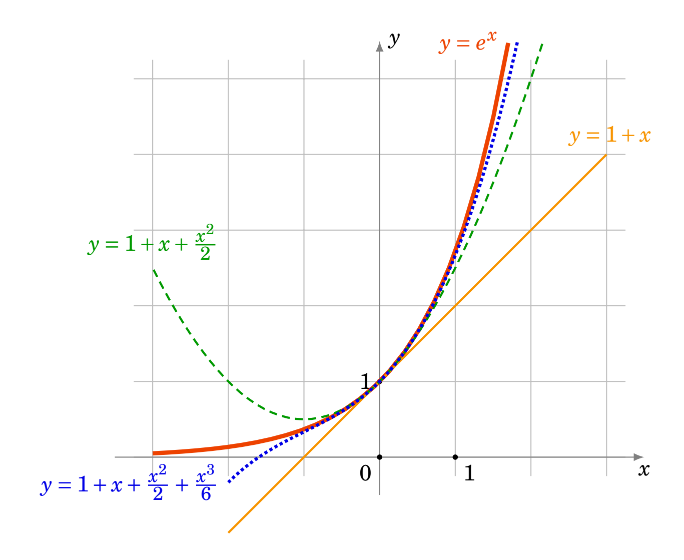
Exo7

13 Développements limités

Vidéo ■ partie 1. Formules de Taylor
Vidéo ■ partie 2. Développements limités au voisinage d'un point
Vidéo ■ partie 3. Opérations sur les DL
Vidéo ■ partie 4. Applications
Exercices ◆ Développements limités

Motivation

Prenons l'exemple de la fonction exponentielle. Une idée du comportement de la fonction $f(x) = \exp x$ autour du point $x = 0$ est donné par sa tangente, dont l'équation est $y = 1 + x$. Nous avons approximé le graphe par une droite. Si l'on souhaite faire mieux, quelle parabole d'équation $y = c_0 + c_1 x + c_2 x^2$ approche le mieux le graphe de f autour de $x = 0$? Il s'agit de la parabole d'équation $y = 1 + x + \frac{1}{2}x^2$. Cette équation à la propriété remarquable que si on note $g(x) = \exp x - \left(1 + x + \frac{1}{2}x^2\right)$ alors $g(0) = 0$, $g'(0) = 0$ et $g''(0) = 0$. Trouver l'équation de cette parabole c'est faire un développement limité à l'ordre 2 de la fonction f. Bien sûr si l'on veut être plus précis, on continuerait avec une courbe du troisième degré qui serait en fait $y = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3$.



Dans ce chapitre, pour n'importe quelle fonction, nous allons trouver le polynôme de degré n qui approche le mieux la fonction. Les résultats ne sont valables que pour x autour d'une valeur fixée (ce sera souvent autour de 0). Ce polynôme sera calculé à partir des dérivées successives au point considéré. Sans plus attendre, voici la formule, dite formule de Taylor-Young :

$$f(x) = f(0) + f'(0)x + f''(0)\frac{x^2}{2!} + \cdots + f^{(n)}(0)\frac{x^n}{n!} + x^n \varepsilon(x).$$

La partie polynomiale $f(0)+f'(0)x+\cdots+f^{(n)}(0)\frac{x^n}{n!}$ est le polynôme de degré n qui approche le mieux $f(x)$ autour de $x=0$. La partie $x^n\varepsilon(x)$ est le «reste» dans lequel $\varepsilon(x)$ est une fonction qui tend vers 0 (quand x tend vers 0) et qui est négligeable devant la partie polynomiale.

1. Formules de Taylor

Nous allons voir trois formules de Taylor, elles auront toutes la même partie polynomiale mais donnent plus ou moins d'informations sur le reste. Nous commencerons par la formule de Taylor avec reste intégral qui donne une expression exacte du reste. Puis la formule de Taylor avec reste $f^{(n+1)}(c)$ qui permet d'obtenir un encadrement du reste et nous terminons avec la formule de Taylor-Young très pratique si l'on n'a pas besoin d'information sur le reste.

Soit $I\subset\mathbb{R}$ un intervalle ouvert. Pour $n\in\mathbb{N}^*$, on dit que $f:I\to\mathbb{R}$ est une fonction de ***classe*** $\mathscr{C}^n$ si f est n fois dérivable sur I et $f^{(n)}$ est continue. f est de ***classe*** $\mathscr{C}^0$ si f est continue sur I. f est de ***classe*** $\mathscr{C}^\infty$ si f est de classe $\mathscr{C}^n$ pour tout $n\in\mathbb{N}$.

1.1. Formule de Taylor avec reste intégral

Théorème 37. Formule de Taylor avec reste intégral

Soit $f:I\to\mathbb{R}$ une fonction de classe $\mathscr{C}^{n+1}$ ($n\in\mathbb{N}$) et soit $a,x\in I$. Alors

$$f(x)=f(a)+f'(a)(x-a)+\frac{f''(a)}{2!}(x-a)^2+\cdots+\frac{f^{(n)}(a)}{n!}(x-a)^n+\int_a^x\frac{f^{(n+1)}(t)}{n!}(x-t)^n\,dt.$$

Nous noterons $T_n(x)$ la partie polynomiale de la formule de Taylor (elle dépend de n mais aussi de f et a) :

$$T_n(x)=f(a)+f'(a)(x-a)+\frac{f''(a)}{2!}(x-a)^2+\cdots+\frac{f^{(n)}(a)}{n!}(x-a)^n.$$

Remarque

En écrivant $x=a+h$ (et donc $h=x-a$) la formule de Taylor précédente devient (pour tout a et $a+h$ de I) :

$$f(a+h)=f(a)+f'(a)h+\frac{f''(a)}{2!}h^2+\cdots+\frac{f^{(n)}(a)}{n!}h^n+\int_0^h\frac{f^{(n+1)}(a+t)}{n!}(h-t)^n\,dt$$

Exemple 129

La fonction $f(x)=\exp x$ est de classe $\mathscr{C}^{n+1}$ sur $I=\mathbb{R}$ pour tout n. Fixons $a\in\mathbb{R}$. Comme $f'(x)=\exp x$, $f''(x)=\exp x$,... alors pour tout $x\in\mathbb{R}$:

$$\exp x=\exp a+\exp a\cdot(x-a)+\cdots+\frac{\exp a}{n!}(x-a)^n+\int_a^x\frac{\exp t}{n!}(x-t)^n\,dt.$$

Bien sûr si l'on se place en $a=0$ alors on retrouve le début de notre approximation de la fonction exponentielle en $x=0$: $\exp x=1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots$

Démonstration . Preuve du théorème

Montrons cette formule de Taylor par récurrence sur $k \leqslant n$:

$$f(b)=f(a)+f'(a)(b-a)+\frac{f''(a)}{2!}(b-a)^2+\cdots+\frac{f^{(k)}(a)}{k!}(b-a)^k+\int_a^b f^{(k+1)}(t)\frac{(b-t)^k}{k!}dt.$$

(Pour éviter les confusions entre ce qui varie et ce qui est fixe dans cette preuve on remplace x par b.)

Initialisation. Pour $n=0$, une primitive de $f'(t)$ est $f(t)$ donc $\int_a^b f'(t)dt = f(b)-f(a)$, donc $f(b)=f(a)+\int_a^b f'(t)dt$. (On rappelle que par convention $(b-t)^0=1$ et $0!=1$.)
Hérédité. Supposons la formule vraie au rang $k-1$. Elle s'écrit $f(b)=f(a)+f'(a)(b-a)+\cdots+\frac{f^{(k-1)}(a)}{(k-1)!}(b-a)^{k-1}+\int_a^b f^{(k)}(t)\frac{(b-t)^{k-1}}{(k-1)!}dt$.
On effectue une intégration par parties dans l'intégrale $\int_a^b f^{(k)}(t)\frac{(b-t)^{k-1}}{(k-1)!}dt$. En posant $u(t)=f^{(k)}(t)$ et $v'(t)=\frac{(b-t)^{k-1}}{(k-1)!}$, on a $u'(t)=f^{(k+1)}(t)$ et $v(t)=-\frac{(b-t)^k}{k!}$; alors

$$\begin{aligned}\int_a^b f^{(k)}(t)\frac{(b-t)^{k-1}}{(k-1)!}dt &= \left[-f^{(k)}(t)\frac{(b-t)^k}{k!}\right]_a^b+\int_a^b f^{(k+1)}(t)\frac{(b-t)^k}{k!}dt\\ &= f^{(k)}(a)\frac{(b-a)^k}{k!}+\int_a^b f^{(k+1)}(t)\frac{(b-t)^k}{k!}dt.\end{aligned}$$

Ainsi lorsque l'on remplace cette expression dans la formule au rang $k-1$ on obtient la formule au rang k.
Conclusion. Par le principe de récurrence la formule de Taylor est vraie pour tous les entiers n pour lesquels f est classe $\mathscr{C}^{n+1}$.

1.2. Formule de Taylor avec reste $f^{(n+1)}(c)$

Théorème 38. Formule de Taylor avec reste $f^{(n+1)}(c)$

Soit $f : I \to \mathbb{R}$ une fonction de classe $\mathscr{C}^{n+1}$ ($n \in \mathbb{N}$) et soit $a, x \in I$. Il existe un réel c entre a et x tel que :

$$f(x)=f(a)+f'(a)(x-a)+\frac{f''(a)}{2!}(x-a)^2+\cdots+\frac{f^{(n)}(a)}{n!}(x-a)^n+\frac{f^{(n+1)}(c)}{(n+1)!}(x-a)^{n+1}.$$

Exemple 130

Soient $a, x \in \mathbb{R}$. Pour tout entier $n \geqslant 0$ il existe c entre a et x tel que $\exp x = \exp a + \exp a \cdot (x-a)+\cdots+\frac{\exp a}{n!}(x-a)^n+\frac{\exp c}{(n+1)!}(x-a)^{n+1}$.

Dans la plupart des cas on ne connaîtra pas ce c. Mais ce théorème permet d'encadrer le reste. Ceci s'exprime par le corollaire suivant :

Corollaire 18

Si en plus la fonction $|f^{(n+1)}|$ est majorée sur I par un réel M, alors pour tout $a, x \in I$, on a :

$$\left|f(x) - T_n(x)\right| \leqslant M \frac{|x-a|^{n+1}}{(n+1)!}.$$

Exemple 131

Approximation de $\sin(0,01)$.
Soit $f(x) = \sin x$. Alors $f'(x) = \cos x$, $f''(x) = -\sin x$, $f^{(3)}(x) = -\cos x$, $f^{(4)}(x) = \sin x$. On obtient donc $f(0) = 0$, $f'(0) = 1$, $f''(0) = 0$, $f^{(3)}(0) = -1$. La formule de Taylor ci-dessus en $a = 0$ à l'ordre 3 devient : $f(x) = 0 + 1 \cdot x + 0 \cdot \frac{x^2}{2!} - 1\frac{x^3}{3!} + f^{(4)}(c)\frac{x^4}{4!}$, c'est-à-dire $f(x) = x - \frac{x^3}{6} + f^{(4)}(c)\frac{x^4}{24}$, pour un certain c entre 0 et x.
Appliquons ceci pour $x = 0,01$. Le reste étant petit on trouve alors

$$\sin(0,01) \approx 0,01 - \frac{(0,01)^3}{6} = 0,00999983333\dots$$

On peut même savoir quelle est la précision de cette approximation : comme $f^{(4)}(x) = \sin x$ alors $|f^{(4)}(c)| \leqslant 1$. Donc $\left|f(x) - \left(x - \frac{x^3}{6}\right)\right| \leqslant \frac{x^4}{4!}$. Pour $x = 0,01$ cela donne : $\left|\sin(0,01) - \left(0,01 - \frac{(0,01)^3}{6}\right)\right| \leqslant \frac{(0,01)^4}{24}$. Comme $\frac{(0,01)^4}{24} \approx 4,16 \cdot 10^{-10}$ alors notre approximation donne au moins 8 chiffres exacts après la virgule.

Remarque

- Dans ce théorème l'hypothèse f de classe $\mathscr{C}^{n+1}$ peut-être affaiblie en f est «$n+1$ fois dérivable sur I».
- «le réel c est entre a et x» signifie «$c \in]a, x[$ ou $c \in]x, a[$».
- Pour $n = 0$ c'est exactement l'énoncé du théorème des accroissements finis : il existe $c \in]a, b[$ tel que $f(b) = f(a) + f'(c)(b-a)$.
- Si I est un intervalle fermé borné et f de classe $\mathscr{C}^{n+1}$, alors $f^{(n+1)}$ est continue sur I donc il existe un M tel que $|f^{(n+1)}(x)| \leqslant M$ pour tout $x \in I$. Ce qui permet toujours d'appliquer le corollaire.

Pour la preuve du théorème nous aurons besoin d'un résultat préliminaire.

Lemme 6. Égalité de la moyenne

Supposons $a < b$ et soient $u, v : [a,b] \to \mathbb{R}$ deux fonctions continues avec $v \geqslant 0$. Alors il existe $c \in [a,b]$ tel que $\int_a^b u(t)v(t)\,dt = u(c)\int_a^b v(t)\,dt$.

Démonstration

Notons $m = \inf_{t\in[a,b]} u(t)$ et $M = \sup_{t\in[a,b]} u(t)$. On a $m\int_a^b v(t)\,dt \leqslant \int_a^b u(t)v(t)\,dt \leqslant M\int_a^b v(t)\,dt$ (car $v \geqslant 0$). Ainsi $m \leqslant \frac{\int_a^b u(t)v(t)\,dt}{\int_a^b v(t)\,dt} \leqslant M$. Puisque u est continue sur $[a,b]$ elle prend toutes les valeurs comprises entre m et M (théorème des valeurs intermédiaires). Donc il existe $c \in [a,b]$ avec $u(c) = \frac{\int_a^b u(t)v(t)\,dt}{\int_a^b v(t)\,dt}$.

Démonstration . Preuve du théorème

Pour la preuve nous montrerons la formule de Taylor pour $f(b)$ en supposant $a < b$. Nous montrerons seulement $c \in [a,b]$ au lieu de $c \in]a,b[$.
Posons $u(t) = f^{(n+1)}(t)$ et $v(t) = \frac{(b-t)^n}{n!}$. La formule de Taylor avec reste intégral s'écrit $f(b) = T_n(a) + \int_a^b u(t)v(t)\,dt$. Par le lemme, il existe $c \in [a,b]$ tel que $\int_a^b u(t)v(t)\,dt = u(c)\int_a^b v(t)\,dt$. Ainsi le reste est $\int_a^b u(t)v(t)\,dt = f^{(n+1)}(c)\int_a^b \frac{(b-t)^n}{n!}\,dt = f^{(n+1)}(c)\left[-\frac{(b-t)^{n+1}}{(n+1)!}\right]_a^b = f^{(n+1)}(c)\frac{(b-a)^{n+1}}{(n+1)!}$. Ce qui donne la formule recherchée.

1.3. Formule de Taylor-Young

Théorème 39. Formule de Taylor-Young

Soit $f : I \to \mathbb{R}$ une fonction de classe $\mathscr{C}^n$ et soit $a \in I$. Alors pour tout $x \in I$ on a :

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n + (x-a)^n\varepsilon(x),$$

où ε est une fonction définie sur I telle que $\varepsilon(x) \xrightarrow[x\to a]{} 0$.

Démonstration

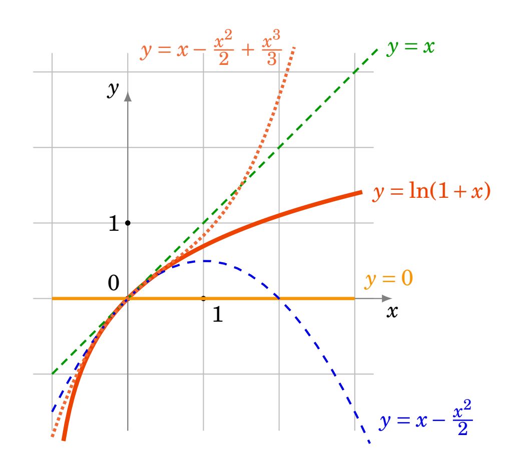
f étant un fonction de classe $\mathscr{C}^n$ nous appliquons la formule de Taylor avec reste $f^{(n)}(c)$ au rang $n-1$. Pour tout x, il existe $c = c(x)$ compris entre a et x tel que $f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n-1)}(a)}{(n-1)!}(x-a)^{n-1} + \frac{f^{(n)}(c)}{n!}(x-a)^n$. Que nous réécrivons : $f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n + \frac{f^{(n)}(c)-f^{(n)}(a)}{n!}(x-a)^n$. On pose $\varepsilon(x) = \frac{f^{(n)}(c)-f^{(n)}(a)}{n!}$. Puisque $f^{(n)}$ est continue et que $c(x) \to a$ alors $\lim_{x\to a}\varepsilon(x) = 0$.

1.4. Un exemple

Soit $f :]-1,+\infty[\to \mathbb{R}$, $x \mapsto \ln(1+x)$; f est infiniment dérivable. Nous allons calculer les formules de Taylor en 0 pour les premiers ordres.
Tous d'abord $f(0) = 0$. Ensuite $f'(x) = \frac{1}{1+x}$ donc $f'(0) = 1$. Ensuite $f''(x) = -\frac{1}{(1+x)^2}$ donc $f''(0) = -1$. Puis $f^{(3)}(x) = +2\frac{1}{(1+x)^3}$ donc $f^{(3)}(0) = +2$. Par récurrence on montre que $f^{(n)}(x) = (-1)^{n-1}(n-1)!\frac{1}{(1+x)^n}$ et donc $f^{(n)}(0) = (-1)^{n-1}(n-1)!$. Ainsi pour $n > 0$: $\frac{f^{(n)}(0)}{n!}x^n = (-1)^{n-1}\frac{(n-1)!}{n!}x^n = (-1)^{n-1}\frac{x^n}{n}$.
Voici donc les premiers polynômes de Taylor :

$$T_0(x) = 0 \qquad T_1(x) = x \qquad T_2(x) = x - \frac{x^2}{2} \qquad T_3(x) = x - \frac{x^2}{2} + \frac{x^3}{3}$$

Les formules de Taylor nous disent que les restes sont de plus en plus petits lorsque n croît. Sur le dessins les graphes des polynômes T_0, T_1, T_2, T_3 s'approchent de plus en plus du graphe de f. Attention ceci n'est vrai qu'autour de 0.



Pour n quelconque nous avons calculer que le polynôme de Taylor en 0 est

$$T_n(x) = \sum_{k=1}^{n}(-1)^{k-1}\frac{x^k}{k} = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots + (-1)^{n-1}\frac{x^n}{n}.$$

1.5. Résumé

Il y a donc trois formules de Taylor qui s'écrivent toutes sous la forme

$$f(x) = T_n(x) + R_n(x)$$

où $T_n(x)$ est toujours le même polynôme de Taylor :

$$T_n(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n.$$

C'est l'expression du reste $R_n(x)$ qui change (attention le reste n'a aucune raison d'être un polynôme).

$$R_n(x) = \int_a^x \frac{f^{(n+1)}(t)}{n!}(x-t)^n dt \qquad \text{Taylor avec reste intégral}$$

$$R_n(x) = \frac{f^{(n+1)}(c)}{(n+1)!}(x-a)^{n+1} \qquad \text{Taylor avec reste } f^{(n+1)}(c),\ c \text{ entre } a \text{ et } x$$

$$R_n(x) = (x-a)^n \varepsilon(x) \qquad \text{Taylor-Young avec } \varepsilon(x) \xrightarrow[x\to a]{} 0$$

Selon les situations l'une des formulations est plus adaptée que les autres. Bien souvent nous n'avons pas besoin de beaucoup d'information sur le reste et c'est donc la formule de Taylor-Young qui sera la plus utile.
Notons que les trois formules ne requièrent pas exactement les mêmes hypothèses : Taylor avec reste intégral à l'ordre n exige une fonction de classe $\mathscr{C}^{n+1}$, Taylor avec reste une fonction $n+1$ fois dérivable, et Taylor-Young une fonction $\mathscr{C}^n$. Une hypothèse plus restrictive donne logiquement une conclusion plus forte. Cela dit, pour les fonctions de classe $\mathscr{C}^\infty$ que l'on manipule le plus souvent, les trois hypothèses sont toujours vérifiées.

Notation. Le terme $(x-a)^n\varepsilon(x)$ où $\varepsilon(x) \xrightarrow[x\to 0]{} 0$ est souvent abrégé en «***petit o***» de $(x-a)^n$ et est noté $o((x-a)^n)$. Donc $o((x-a)^n)$ est une fonction telle que $\lim_{x\to a} \frac{o((x-a)^n)}{(x-a)^n} = 0$. Il faut s'habituer à cette notation qui simplifie les écritures, mais il faut toujours garder à l'esprit ce qu'elle signifie.

Cas particulier : Formule de Taylor-Young au voisinage de 0. On se ramène souvent au cas particulier où $a = 0$, la formule de Taylor-Young s'écrit alors

$$\boxed{f(x) = f(0) + f'(0)x + f''(0)\frac{x^2}{2!} + \cdots + f^{(n)}(0)\frac{x^n}{n!} + x^n\varepsilon(x)}$$

où $\lim_{x\to 0}\varepsilon(x) = 0$.
Et avec la notation «petit o» cela donne :

$$f(x) = f(0) + f'(0)x + f''(0)\frac{x^2}{2!} + \cdots + f^{(n)}(0)\frac{x^n}{n!} + o(x^n)$$

Mini-exercices

1. Écrire les trois formules de Taylor en 0 pour $x \mapsto \cos x$, $x \mapsto \exp(-x)$ et $x \mapsto \operatorname{sh} x$.
2. Écrire les formules de Taylor en 0 à l'ordre 2 pour $x \mapsto \frac{1}{\sqrt{1+x}}$, $x \mapsto \tan x$.
3. Écrire les formules de Taylor en 1 pour $x \mapsto x^3 - 9x^2 + 14x + 3$.

4. Avec une formule de Taylor à l'ordre 2 de $\sqrt{1+x}$, trouver une approximation de $\sqrt{1,01}$. Idem avec $\ln(0,99)$.

2. Développements limités au voisinage d'un point

2.1. Définition et existence

Soit I un intervalle ouvert et $f : I \to \mathbb{R}$ une fonction quelconque.

Définition 67

Pour $a \in I$ et $n \in \mathbb{N}$, on dit que f admet un ***développement limité*** (***DL***) au point a et à l'ordre n, s'il existe des réels $c_0, c_1, \dots, c_n$ et une fonction $\varepsilon : I \to \mathbb{R}$ telle que $\lim_{x \to a} \varepsilon(x) = 0$ de sorte que pour tout $x \in I$:

$$f(x) = c_0 + c_1(x-a) + \cdots + c_n(x-a)^n + (x-a)^n \varepsilon(x).$$

- L'égalité précédente s'appelle un DL de f au voisinage de a à l'ordre n .
- Le terme $c_0 + c_1(x-a) + \cdots + c_n(x-a)^n$ est appelé la ***partie polynomiale*** du DL.
- Le terme $(x-a)^n \varepsilon(x)$ est appelé le ***reste*** du DL.

La formule de Taylor-Young permet d'obtenir immédiatement des développements limités en posant $c_k = \frac{f^{(k)}(a)}{k!}$:

Proposition 84

Si f est de classe $\mathscr{C}^n$ au voisinage d'un point a alors f admet un DL au point a à l'ordre n, qui provient de la formule de Taylor-Young :

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n + (x-a)^n \varepsilon(x)$$

où $\lim_{x \to a} \varepsilon(x) = 0$.

Remarque

1. Si f est de classe $\mathscr{C}^n$ au voisinage d'un point 0, un DL en 0 à l'ordre n est l'expression :

$$f(x) = f(0) + f'(0)x + f''(0)\frac{x^2}{2!} + \cdots + f^{(n)}(0)\frac{x^n}{n!} + x^n \varepsilon(x)$$

2. Si f admet un DL en un point a à l'ordre n alors elle en possède un pour tout $k \leqslant n$. En effet

$$\begin{aligned} f(x) &= f(a) + \frac{f'(a)}{1!}(x-a) + \cdots + \frac{f^{(k)}(a)}{k!}(x-a)^k \\ &\quad + \underbrace{\frac{f^{(k+1)}(a)}{(k+1)!}(x-a)^{k+1} + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n + (x-a)^n \varepsilon(x)}_{=(x-a)^k \eta(x)} \end{aligned}$$

où $\lim_{x \to a} \eta(x) = 0$.

2.2. Unicité

Proposition 85

Si f admet un DL alors ce DL est unique.

Démonstration

Écrivons deux DL de f : $f(x) = c_0 + c_1(x-a) + \cdots + c_n(x-a)^n + (x-a)^n \varepsilon_1(x)$ et $f(x) = d_0 + d_1(x-a) + \cdots + d_n(x-a)^n + (x-a)^n \varepsilon_2(x)$. En effectuant la différence on obtient :

$$(d_0 - c_0) + (d_1 - c_1)(x-a) + \cdots + (d_n - c_n)(x-a)^n + (x-a)^n(\varepsilon_2(x) - \varepsilon_1(x)) = 0.$$

Lorsque l'on fait $x = a$ dans cette égalité alors on trouve $d_0 - c_0 = 0$. Ensuite on peut diviser cette égalité par $x-a$: $(d_1 - c_1) + (d_2 - c_2)(x-a) + \cdots + (d_n - c_n)(x-a)^{n-1} + (x-a)^{n-1}(\varepsilon_2(x) - \varepsilon_1(x)) = 0$. En évaluant en $x = a$ on obtient $d_1 - c_1 = 0$, etc. On trouve $c_0 = d_0$, $c_1 = d_1$, ..., $c_n = d_n$. Les parties polynomiales sont égales et donc les restes aussi.

Corollaire 19

Si f est paire (resp. impaire) alors la partie polynomiale de son DL en 0 ne contient que des monômes de degrés pairs (resp. impairs).

Par exemple $x \mapsto \cos x$ est paire et nous verrons que son DL en 0 commence par : $\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots$.

Démonstration

$f(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \cdots + c_n x^n + x^n \varepsilon(x)$. Si f est paire alors $f(x) = f(-x) = c_0 - c_1 x + c_2 x^2 - c_3 x^3 + \cdots + (-1)^n c_n x^n + x^n \varepsilon(x)$. Par l'unicité du DL en 0 on trouve $c_1 = -c_1$, $c_3 = -c_3$, ... et donc $c_1 = 0$, $c_3 = 0$,...

Remarque

1. L'unicité du DL et la formule de Taylor-Young prouve que si l'on connaît le DL et que f est de classe $\mathscr{C}^n$ alors on peut calculer les nombres dérivés à partir de la partie polynomiale par la formule $c_k = \frac{f^{(k)}(a)}{k!}$. Cependant dans la majorité des cas on fera l'inverse : on trouve le DL à partir des dérivées.
2. Si f admet un DL en un point a à l'ordre $n \geqslant 0$ alors $c_0 = f(a)$.
3. Si f admet un DL en un point a à l'ordre $n \geqslant 1$, alors f est dérivable en a et on a $c_0 = f(a)$ et $c_1 = f'(a)$. Par conséquent $y = c_0 + c_1(x-a)$ est l'équation de la tangente au graphe de f au point d'abscisse a.
4. Plus subtil : f peut admettre un DL à l'ordre 2 en un point a *sans* admettre une dérivée seconde en a. Soit par exemple $f(x) = x^3 \sin \frac{1}{x}$. Alors f est dérivable mais f' ne l'est pas. Pourtant f admet un DL en 0 à l'ordre 2 : $f(x) = x^2 \varepsilon(x)$ (la partie polynomiale est nulle).

2.3. DL des fonctions usuelles à l'origine

Les DL suivants en 0 proviennent de la formule de Taylor-Young.

$$\boxed{\exp x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!} + x^n \varepsilon(x)}$$

$$\operatorname{ch} x = 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots + \frac{x^{2n}}{(2n)!} + x^{2n+1}\varepsilon(x)$$
$$\operatorname{sh} x = \frac{x}{1!} + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots + \frac{x^{2n+1}}{(2n+1)!} + x^{2n+2}\varepsilon(x)$$
$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots + (-1)^n \frac{x^{2n}}{(2n)!} + x^{2n+1}\varepsilon(x)$$
$$\sin x = \frac{x}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots + (-1)^n \frac{x^{2n+1}}{(2n+1)!} + x^{2n+2}\varepsilon(x)$$

$$\boxed{\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots + (-1)^{n-1}\frac{x^n}{n} + x^n\varepsilon(x)}$$

$$\boxed{(1+x)^\alpha = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2!}x^2 + \cdots + \frac{\alpha(\alpha-1)\ldots(\alpha-n+1)}{n!}x^n + x^n\varepsilon(x)}$$

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots + (-1)^n x^n + x^n\varepsilon(x)$$
$$\frac{1}{1-x} = 1 + x + x^2 + \cdots + x^n + x^n\varepsilon(x)$$
$$\sqrt{1+x} = 1 + \frac{x}{2} - \frac{1}{8}x^2 + \cdots + (-1)^{n-1}\frac{1\cdot1\cdot3\cdot5\cdots(2n-3)}{2^n n!}x^n + x^n\varepsilon(x)$$

Ils sont tous à apprendre par cœur. C'est facile avec les remarques suivantes :

- Le DL de $\operatorname{ch} x$ est la partie paire du DL de $\exp x$. C'est-à-dire que l'on ne retient que les monômes de degré pair. Alors que le DL de $\operatorname{sh} x$ est la partie impaire.
- Le DL de $\cos x$ est la partie paire du DL de $\exp x$ en alternant le signe $+/-$ du monôme. Pour $\sin x$ c'est la partie impaire de $\exp x$ en alternant aussi les signes.
- On notera que la précision du DL de $\sin x$ est meilleure que l'application naïve de la formule de Taylor le prévoit ($x^{2n+2}\varepsilon(x)$ au lieu de $x^{2n+1}\varepsilon(x)$) ; c'est parce que le DL est en fait à l'ordre $2n+2$, avec un terme polynomial en x^{2n+2} nul (donc absent). Le même phénomène est vrai pour tous les DL pairs ou impairs (dont $\operatorname{sh} x, \cos x, \operatorname{ch} x$).
- Pour $\ln(1+x)$ n'oubliez pas qu'il n'y a pas de terme constant, pas de factorielle aux dénominateurs, et que les signes alternent.
- Il faut aussi savoir écrire le DL à l'aide des sommes formelles (et ici des «petits o») :

$$\exp x = \sum_{k=1}^{n} \frac{x^k}{k!} + o(x^n) \qquad \text{et} \qquad \ln(1+x) = \sum_{k=1}^{n} (-1)^{k-1}\frac{x^k}{k} + o(x^n)$$

- La DL de $(1+x)^\alpha$ est valide pour tout $\alpha \in \mathbb{R}$. Pour $\alpha = -1$ on retombe sur le DL de $(1+x)^{-1} = \frac{1}{1+x}$. Mais on retient souvent le DL de $\frac{1}{1-x}$ qui est très facile. Il se retrouve aussi avec la somme d'une suite géométrique : $1 + x + x^2 + \cdots + x^n = \frac{1-x^{n+1}}{1-x} = \frac{1}{1-x} - \frac{x^{n+1}}{1-x} = \frac{1}{1-x} + x^n\varepsilon(x)$.
- Pour $\alpha = \frac{1}{2}$ on retrouve $(1+x)^{\frac{1}{2}} = \sqrt{1+x} = 1 + \frac{x}{2} - \frac{1}{8}x^2 + \cdots$. Dont il faut connaître les trois premiers termes.

2.4. DL des fonctions en un point quelconque

La fonction f admet un DL au voisinage d'un point a si et seulement si la fonction $x \mapsto f(x+a)$ admet un DL au voisinage de 0. Souvent on ramène donc le problème en 0 en faisant le changement de variables $h = x - a$.

Exemple 132

1. DL de $f(x) = \exp x$ en 1.

   On pose $h = x - 1$. Si x est proche de 1 alors h est proche de 0. Nous allons nous ramener

à un DL de $\exp h$ en $h=0$. On note $e=\exp 1$.

$$\begin{aligned}\exp x &= \exp(1+(x-1)) = \exp(1)\exp(x-1) = e\exp h = e\left(1+h+\frac{h^2}{2!}+\cdots+\frac{h^n}{n!}+h^n\varepsilon(h)\right)\\ &= e\left(1+(x-1)+\frac{(x-1)^2}{2!}+\cdots+\frac{(x-1)^n}{n!}+(x-1)^n\varepsilon(x-1)\right), \quad \lim_{x\to 1}\varepsilon(x-1)=0.\end{aligned}$$

2. DL de $g(x)=\sin x$ en $\pi/2$.
   Sachant $\sin x = \sin(\frac{\pi}{2}+x-\frac{\pi}{2}) = \cos(x-\frac{\pi}{2})$ on se ramène au DL de $\cos h$ quand $h=x-\frac{\pi}{2}\to 0$.
   On a donc $\sin x = 1-\frac{(x-\frac{\pi}{2})^2}{2!}+\cdots+(-1)^n\frac{(x-\frac{\pi}{2})^{2n}}{(2n)!}+(x-\frac{\pi}{2})^{2n+1}\varepsilon(x-\frac{\pi}{2})$, où $\lim_{x\to\pi/2}\varepsilon(x-\frac{\pi}{2})=0$.
3. DL de $\ell(x)=\ln(1+3x)$ en 1 à l'ordre 3.
   Il faut se ramener à un DL du type $\ln(1+h)$ en $h=0$. On pose $h=x-1$ (et donc $x=1+h$).
   On a $\ell(x)=\ln(1+3x)=\ln\big(1+3(1+h)\big)=\ln(4+3h)=\ln\big(4\cdot(1+\frac{3h}{4})\big)=\ln 4+\ln\big(1+\frac{3h}{4}\big)=$ $\ln 4+\frac{3h}{4}-\frac{1}{2}\big(\frac{3h}{4}\big)^2+\frac{1}{3}\big(\frac{3h}{4}\big)^3+h^3\varepsilon(h)=\ln 4+\frac{3(x-1)}{4}-\frac{9}{32}(x-1)^2+\frac{9}{64}(x-1)^3+(x-1)^3\varepsilon(x-1)$ où $\lim_{x\to1}\varepsilon(x-1)=0$.

Mini-exercices

1. Calculer le DL en 0 de $x\mapsto \operatorname{ch} x$ par la formule de Taylor-Young. Retrouver ce DL en utilisant que $\operatorname{ch} x=\frac{e^x-e^{-x}}{2}$.
2. Écrire le DL en 0 à l'ordre 3 de $\sqrt[3]{1+x}$. Idem avec $\frac{1}{\sqrt{1+x}}$.
3. Écrire le DL en 2 à l'ordre 2 de $\sqrt{x}$.
4. Justifier l'expression du DL de $\frac{1}{1-x}$ à l'aide de l'unicité des DL de la somme d'une suite géométrique.

3. Opérations sur les développements limités

3.1. Somme et produit

On suppose que f et g sont deux fonctions qui admettent des DL en 0 à l'ordre n :

$$f(x)=c_0+c_1x+\cdots+c_nx^n+x^n\varepsilon_1(x) \qquad g(x)=d_0+d_1x+\cdots+d_nx^n+x^n\varepsilon_2(x)$$

Proposition 86

– $f+g$ admet un DL en 0 l'ordre n qui est :

$$(f+g)(x)=f(x)+g(x)=(c_0+d_0)+(c_1+d_1)x+\cdots+(c_n+d_n)x^n+x^n\varepsilon(x).$$

– $f\times g$ admet un DL en 0 l'ordre n qui est : $(f\times g)(x)=f(x)\times g(x)=T_n(x)+x^n\varepsilon(x)$ où $T_n(x)$ est le polynôme $(c_0+c_1x+\cdots+c_nx^n)\times(d_0+d_1x+\cdots+d_nx^n)$ tronqué à l'ordre n.

Tronquer un polynôme à l'ordre n signifie que l'on conserve seulement les monômes de degré $\leqslant n$.

Exemple 133

Calculer le DL de $\cos x \times \sqrt{1+x}$ en 0 à l'ordre 2. On sait $\cos x = 1 - \frac{1}{2}x^2 + x^2\varepsilon_1(x)$ et $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + x^2\varepsilon_2(x)$. Donc :

$$\begin{aligned}
\cos x \times \sqrt{1+x} &= \left(1 - \frac{1}{2}x^2 + x^2\varepsilon_1(x)\right) \times \left(1 + \frac{1}{2}x - \frac{1}{8}x^2 + x^2\varepsilon_2(x)\right) \quad \text{on développe} \\
&= 1 + \frac{1}{2}x - \frac{1}{8}x^2 + x^2\varepsilon_2(x) \\
&\quad - \frac{1}{2}x^2\left(1 + \frac{1}{2}x - \frac{1}{8}x^2 + x^2\varepsilon_2(x)\right) \\
&\quad + x^2\varepsilon_1(x)\left(1 + \frac{1}{2}x - \frac{1}{8}x^2 + x^2\varepsilon_2(x)\right) \\
&= 1 + \frac{1}{2}x - \frac{1}{8}x^2 + x^2\varepsilon_2(x) \quad \text{on développe encore} \\
&\quad - \frac{1}{2}x^2 - \frac{1}{4}x^3 + \frac{1}{16}x^4 - \frac{1}{2}x^4\varepsilon_2(x) \\
&\quad + x^2\varepsilon_1(x) + \frac{1}{2}x^3\varepsilon_1(x) - \frac{1}{8}x^4\varepsilon_1(x) + x^4\varepsilon_1(x)\varepsilon_2(x) \\
&= \underbrace{1 + \frac{1}{2}x + \left(-\frac{1}{8}x^2 - \frac{1}{2}x^2\right)}_{\text{partie tronquée à l'ordre 2}} \quad \text{on a regroupé les termes de degré 0 et 1, 2} \\
&\quad \underbrace{+ x^2\varepsilon_2(x) - \frac{1}{4}x^3 + \frac{1}{16}x^4 - \frac{1}{2}x^4\varepsilon_2(x) + x^2\varepsilon_1(x) + \frac{1}{2}x^3\varepsilon_1(x) - \frac{1}{8}x^4\varepsilon_1(x) + x^4\varepsilon_1(x)\varepsilon_2(x)}_{\text{reste de la forme } x^2\varepsilon(x)} \quad \text{et ici les aut} \\
&= 1 + \frac{1}{2}x - \frac{5}{8}x^2 + x^2\varepsilon(x)
\end{aligned}$$

On a en fait écrit beaucoup de choses superflues, qui à la fin sont dans le reste et n'avaient pas besoin d'être explicitées ! Avec l'habitude les calculs se font très vite car on n'écrit plus les termes inutiles. Voici le même calcul avec la notation «petit o» : dès qu'apparaît un terme $x^2\varepsilon_1(x)$ ou un terme x^3,... on écrit juste $o(x^2)$ (ou si l'on préfère $x^2\varepsilon(x)$).

$$\begin{aligned}
\cos x \times \sqrt{1+x} &= \left(1 - \frac{1}{2}x^2 + o(x^2)\right) \times \left(1 + \frac{1}{2}x - \frac{1}{8}x^2 + o(x^2)\right) \quad \text{on développe} \\
&= 1 + \frac{1}{2}x - \frac{1}{8}x^2 + o(x^2) \\
&\quad - \frac{1}{2}x^2 + o(x^2) \\
&\quad + o(x^2) \\
&= 1 + \frac{1}{2}x - \frac{5}{8}x^2 + o(x^2)
\end{aligned}$$

La notation «petit o» évite de devoir donner un nom à chaque fonction, en ne gardant que sa propriété principale, qui est de décroître vers 0 au moins à une certaine vitesse. Comme on le voit dans cet exemple, $o(x^2)$ *absorbe* les éléments de même ordre de grandeur ou plus petits que lui : $o(x^2) - \frac{1}{4}x^3 + \frac{1}{2}x^2 o(x^2) = o(x^2)$. Mais il faut bien comprendre que les différents $o(x^2)$ écrits ne correspondent pas à la même fonction, ce qui justifie que cette égalité ne soit pas fausse !

3.2. Composition

On écrit encore :

$$f(x) = C(x) + x^n\varepsilon_1(x) = c_0 + c_1x + \cdots + c_nx^n + x^n\varepsilon_1(x) \qquad g(x) = D(x) + x^n\varepsilon_2(x) = d_0 + d_1x + \cdots + d_nx^n + x^n\varepsilon_2(x)$$

Proposition 87

Si $g(0) = 0$ (c'est-à-dire $d_0 = 0$) alors la fonction $f \circ g$ admet un DL en 0 à l'ordre n dont la partie polynomiale est le polynôme tronqué à l'ordre n de la composition $C(D(x))$.

Exemple 134

Calcul du DL de $h(x) = \sin\big(\ln(1+x)\big)$ en 0 à l'ordre 3.
- On pose ici $f(u) = \sin u$ et $g(x) = \ln(1+x)$ (pour plus de clarté il est préférable de donner des noms différents aux variables de deux fonctions, ici x et u). On a bien $f \circ g(x) = \sin\big(\ln(1+x)\big)$ et $g(0) = 0$.
- On écrit le DL à l'ordre 3 de $f(u) = \sin u = u - \frac{u^3}{3!} + u^3\varepsilon_1(u)$ pour u proche de 0.
- Et on pose $u = g(x) = \ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + x^3\varepsilon_2(x)$ pour x proche de 0.
- On aura besoin de calculer un DL à l'ordre 3 de u^2 (qui est bien sûr le produit $u \times u$) : $u^2 = \big(x - \frac{x^2}{2} + \frac{x^3}{3} + x^3\varepsilon_2(x)\big)^2 = x^2 - x^3 + x^3\varepsilon_3(x)$ et aussi u^3 qui est $u \times u^2$, $u^3 = x^3 + x^3\varepsilon_4(x)$.
- Donc $h(x) = f \circ g(x) = f(u) = u - \frac{u^3}{3!} + u^3\varepsilon_1(u) = \big(x - \frac{1}{2}x^2 + \frac{1}{3}x^3\big) - \frac{1}{6}x^3 + x^3\varepsilon(x) = x - \frac{1}{2}x^2 + \frac{1}{6}x^3 + x^3\varepsilon(x)$.

Exemple 135

Soit $h(x) = \sqrt{\cos x}$. On cherche le DL de h en 0 à l'ordre 4.
On utilise cette fois la notation «petit o». On connaît le DL de $f(u) = \sqrt{1+u}$ en $u = 0$ à l'ordre 2 : $f(u) = \sqrt{1+u} = 1 + \frac{1}{2}u - \frac{1}{8}u^2 + o(u^2)$.
Et si on pose $u(x) = \cos x - 1$ alors on a $h(x) = f\big(u(x)\big)$ et $u(0) = 0$. D'autre part le DL de $u(x)$ en $x = 0$ à l'ordre 4 est : $u = -\frac{1}{2}x^2 + \frac{1}{24}x^4 + o(x^4)$. On trouve alors $u^2 = \frac{1}{4}x^4 + o(x^4)$.
Et ainsi

$$\begin{aligned}
h(x) = f\big(u\big) &= 1 + \frac{1}{2}u - \frac{1}{8}u^2 + o(u^2) \\
&= 1 + \frac{1}{2}\Big(-\frac{1}{2}x^2 + \frac{1}{24}x^4\Big) - \frac{1}{8}\Big(\frac{1}{4}x^4\Big) + o(x^4) \\
&= 1 - \frac{1}{4}x^2 + \frac{1}{48}x^4 - \frac{1}{32}x^4 + o(x^4) \\
&= 1 - \frac{1}{4}x^2 - \frac{1}{96}x^4 + o(x^4)
\end{aligned}$$

3.3. Division

Voici comment calculer le DL d'un quotient f/g. Soient

$$f(x) = c_0 + c_1x + \cdots + c_nx^n + x^n\varepsilon_1(x) \qquad g(x) = d_0 + d_1x + \cdots + d_nx^n + x^n\varepsilon_2(x)$$

Nous allons utiliser le DL de $\frac{1}{1+u} = 1 - u + u^2 - u^3 + \cdots$.

1. Si $d_0 = 1$ on pose $u = d_1 x + \cdots + d_n x^n + x^n \varepsilon_2(x)$ et le quotient s'écrit $f/g = f \times \frac{1}{1+u}$.
2. Si d_0 est quelconque avec $d_0 \neq 0$ alors on se ramène au cas précédent en écrivant

$$\frac{1}{g(x)} = \frac{1}{d_0} \frac{1}{1 + \frac{d_1}{d_0} x + \cdots + \frac{d_n}{d_0} x^n + \frac{x^n \varepsilon_2(x)}{d_0}}.$$

3. Si $d_0 = 0$ alors on factorise par x^k (pour un certain k) afin de se ramener aux cas précédents.

Exemple 136

1. DL de $\tan x$ en 0 à l'ordre 5.

   Tout d'abord $\sin x = x - \frac{x^3}{6} + \frac{x^5}{120} + x^5 \varepsilon(x)$. D'autre part $\cos x = 1 - \frac{x^2}{2} + \frac{x^4}{24} + x^5 \varepsilon(x) = 1 + u$ en posant $u = -\frac{x^2}{2} + \frac{x^4}{24} + x^5 \varepsilon(x)$.

   Nous aurons besoin de u^2 et u^3 : $u^2 = \left(-\frac{x^2}{2} + \frac{x^4}{24} + x^5 \varepsilon(x)\right)^2 = \frac{x^4}{4} + x^5 \varepsilon(x)$ et en fait $u^3 = x^5 \varepsilon(x)$. (On note abusivement $\varepsilon(x)$ pour différents restes.)

   Ainsi

   $$\frac{1}{\cos x} = \frac{1}{1+u} = 1 - u + u^2 - u^3 + u^3 \varepsilon(u) = 1 + \frac{x^2}{2} - \frac{x^4}{24} + \frac{x^4}{4} + x^5 \varepsilon(x) = 1 + \frac{x^2}{2} + \frac{5}{24} x^4 + x^5 \varepsilon(x);$$

   Finalement

   $$\tan x = \sin x \times \frac{1}{\cos x} = \left(x - \frac{x^3}{6} + \frac{x^5}{120} + x^5 \varepsilon(x)\right) \times \left(1 + \frac{x^2}{2} + \frac{5}{24} x^4 + x^5 \varepsilon(x)\right) = x + \frac{x^3}{3} + \frac{2}{15} x^5 + x^5 \varepsilon(x).$$

2. DL de $\frac{1+x}{2+x}$ en 0 à l'ordre 4.

   $$\frac{1+x}{2+x} = (1+x)\frac{1}{2}\frac{1}{1+\frac{x}{2}} = \frac{1}{2}(1+x)\left(1 - \frac{x}{2} + \left(\frac{x}{2}\right)^2 - \left(\frac{x}{2}\right)^3 + \left(\frac{x}{2}\right)^4 + o(x^4)\right) = \frac{1}{2} + \frac{x}{4} - \frac{x^2}{8} + \frac{x^3}{16} - \frac{x^4}{32} + o(x^4)$$

3. Si l'on souhaite calculer le DL de $\frac{\sin x}{\operatorname{sh} x}$ en 0 à l'ordre 4 alors on écrit

   $$\begin{aligned}\frac{\sin x}{\operatorname{sh} x} &= \frac{x - \frac{x^3}{3!} + \frac{x^5}{5!} + o(x^5)}{x + \frac{x^3}{3!} + \frac{x^5}{5!} + o(x^5)} = \frac{x\left(1 - \frac{x^2}{3!} + \frac{x^4}{5!} + o(x^4)\right)}{x\left(1 + \frac{x^2}{3!} + \frac{x^4}{5!} + o(x^4)\right)} \\ &= \left(1 - \frac{x^2}{3!} + \frac{x^4}{5!} + o(x^4)\right) \times \frac{1}{1 + \frac{x^2}{3!} + \frac{x^4}{5!} + o(x^4)} = \cdots = 1 - \frac{x^2}{2} + \frac{x^4}{18} + o(x^4)\end{aligned}$$

Autre méthode. Soit $f(x) = C(x) + x^n \varepsilon_1(x)$ et $g(x) = D(x) + x^n \varepsilon_2(x)$. Alors on écrit la division suivant les puissances croissantes de C par D à l'ordre n : $C = DQ + x^{n+1} R$ avec $\deg Q \leqslant n$. Alors Q est la partie polynomiale du DL en 0 à l'ordre n de f/g.

Exemple 137

DL de $\frac{2+x+2x^3}{1+x^2}$ à l'ordre 2. On pose $C(x) = 2 + x + 2x^3$ et $g(x) = D(x) = 1 + x^2$ alors $C(x) = D(x) \times (2 + x - 2x^2) + x^3(1 + 2x)$. On a donc $Q(x) = 2 + x - 2x^2$, $R(x) = 1 + 2x$. Et donc lorsque l'on divise cette égalité par $C(x)$ on obtient $\frac{f(x)}{g(x)} = 2 + x - 2x^2 + x^2 \varepsilon(x)$.

3.4. Intégration

Soit $f : I \to \mathbb{R}$ une fonction de classe $\mathscr{C}^n$ dont le DL en $a \in I$ à l'ordre n est $f(x) = c_0 + c_1(x-a) + c_2(x-a)^2 + \cdots + c_n(x-a)^n + (x-a)^n \varepsilon(x)$.

Théorème 40

Notons F une primitive de f. Alors F admet un DL en a à l'ordre $n+1$ qui s'écrit :

$$F(x)=F(a)+c_0(x-a)+c_1\frac{(x-a)^2}{2}+c_2\frac{(x-a)^3}{3}+\cdots+c_n\frac{(x-a)^{n+1}}{n+1}+(x-a)^{n+1}\eta(x)$$

où $\lim_{x\to a}\eta(x)=0$.

Cela signifie que l'on intègre la partie polynomiale terme à terme pour obtenir le DL de $F(x)$ à la constante $F(a)$ près.

Démonstration

On a $F(x)-F(a)=\int_a^x f(t)dt=a_0(x-a)+\cdots+\frac{a_n}{n+1}(x-a)^{n+1}+\int_a^x(t-a)^{n+1}\varepsilon(t)dt$. Notons $\eta(x)=\frac{1}{(x-a)^{n+1}}\int_a^x(t-a)^n\varepsilon(t)dt$.
Alors $|\eta(x)|\leqslant\left|\frac{1}{(x-a)^{n+1}}\int_a^x|(t-a)^n|\cdot\sup_{t\in[a,x]}|\varepsilon(t)|dt\right|=\left|\frac{1}{(x-a)^{n+1}}\right|\cdot\sup_{t\in[a,x]}|\varepsilon(t)|\cdot\int_a^x|(t-a)^n|dt=\frac{1}{n+1}\sup_{t\in[a,x]}|\varepsilon(t)|$.
Mais $\sup_{t\in[a,x]}|\varepsilon(t)|\to0$ lorsque $x\to a$. Donc $\eta(x)\to0$ quand $x\to a$.

Exemple 138

Calcul du DL de $\arctan x$.
On sait que $\arctan' x=\frac{1}{1+x^2}$. En posant $f(x)=\frac{1}{1+x^2}$ et $F(x)=\arctan x$, on écrit

$$\arctan' x=\frac{1}{1+x^2}=\sum_{k=0}^{n}(-1)^k x^{2k}+x^{2n}\varepsilon(x).$$

Et comme $\arctan(0)=0$ alors $\arctan x=\sum_{k=0}^n\frac{(-1)^k}{2k+1}x^{2k+1}+x^{2n+1}\varepsilon(x)=x-\frac{x^3}{3}+\frac{x^5}{5}-\frac{x^7}{7}+\cdots$

Exemple 139

La méthode est la même pour obtenir un DL de $\arcsin x$ en 0 à l'ordre 5.
$\arcsin' x=(1-x^2)^{-\frac12}=1-\frac12(-x^2)+\frac{-\frac12(-\frac12-1)}{2}(-x^2)^2+x^4\varepsilon(x)=1+\frac12x^2+\frac38x^4+x^4\varepsilon(x)$.
Donc $\arcsin x=x+\frac16x^3+\frac{3}{40}x^5+x^5\varepsilon(x)$.

Mini-exercices

1. Calculer le DL en 0 à l'ordre 3 de $\exp(x)-\frac{1}{1+x}$, puis de $x\cos(2x)$ et $\cos(x)\times\sin(2x)$.
2. Calculer le DL en 0 à l'ordre 2 de $\sqrt{1+2\cos x}$, puis de $\exp\left(\sqrt{1+2\cos x}\right)$.
3. Calculer le DL en 0 à l'ordre 3 de $\ln(1+\sin x)$. Idem à l'ordre 6 pour $\left(\ln(1+x^2)\right)^2$.
4. Calculer le DL en 0 à l'ordre n de $\frac{\ln(1+x^3)}{x^3}$. Idem à l'ordre 3 avec $\frac{e^x}{1+x}$.
5. Par intégration retrouver la formule du DL de $\ln(1+x)$. Idem à l'ordre 3 pour $\arccos x$.

4. Applications des développements limités

Voici les applications les plus remarquables des développements limités. On utilisera aussi les DL lors de l'étude locale des courbes paramétrées lorsqu'il y a des points singuliers.

4.1. Calculs de limites

Les DL sont très efficaces pour calculer des limites ayant des formes indéterminées ! Il suffit juste de remarquer que si $f(x) = c_0 + c_1(x-a) + \cdots$ alors $\lim_{x\to a} f(x) = c_0$.

Exemple 140

Limite en 0 de $\dfrac{\ln(1+x) - \tan x + \frac{1}{2}\sin^2 x}{3x^2 \sin^2 x}$.

Notons $\frac{f(x)}{g(x)}$ cette fraction. En 0 on a $f(x) = \ln(1+x) - \tan x + \frac{1}{2}\sin^2 x = \left(x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + o(x^4)\right) - \left(x + \frac{x^3}{3} + o(x^4)\right) + \frac{1}{2}\left(x - \frac{x^3}{6} + o(x^3)\right)^2 = -\frac{x^2}{2} - \frac{x^4}{4} + \frac{1}{2}(x^2 - \frac{1}{3}x^4) + o(x^4) = -\frac{5}{12}x^4 + o(x^4)$ et $g(x) = 3x^2 \sin^2 x = 3x^2\left(x + o(x)\right)^2 = 3x^4 + o(x^4)$.

Ainsi $\frac{f(x)}{g(x)} = \frac{-\frac{5}{12}x^4 + o(x^4)}{3x^4 + o(x^4)} = \frac{-\frac{5}{12} + o(1)}{3 + o(1)}$ en notant $o(1)$ une fonction (inconnue) tendant vers 0 quand $x \to 0$. Donc $\lim_{x\to 0} \frac{f(x)}{g(x)} = -\frac{5}{36}$.

Note : en calculant le DL à un ordre inférieur (2 par exemple), on n'aurait pas pu conclure, car on aurait obtenu $\frac{f(x)}{g(x)} = \frac{o(x^2)}{o(x^2)}$, ce qui ne lève pas l'indétermination. De façon générale, on calcule les DL à l'ordre le plus bas possible, et si cela ne suffit pas, on augmente progressivement l'ordre (donc la précision de l'approximation).

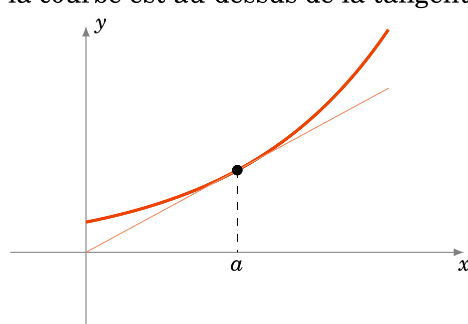
4.2. Position d'une courbe par rapport à sa tangente

Proposition 88

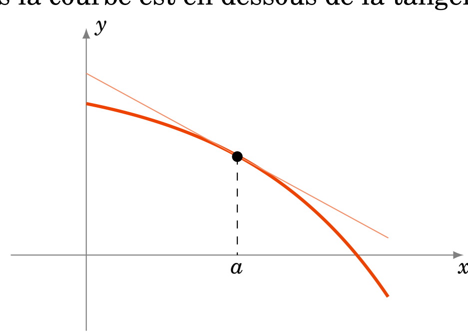
Soit $f : I \to \mathbb{R}$ une fonction admettant un DL en a : $f(x) = c_0 + c_1(x-a) + c_k(x-a)^k + (x-a)^k \varepsilon(x)$, où k est le plus petit entier $\geqslant 2$ tel que le coefficient c_k soit non nul. Alors l'équation de la tangente à la courbe de f en a est : $y = c_0 + c_1(x-a)$ et la position de la courbe par rapport à la tangente pour x proche de a est donnée par le signe $f(x) - y$, c'est-à-dire le signe de $c_k(x-a)^k$.

Il y a 3 cas possibles.

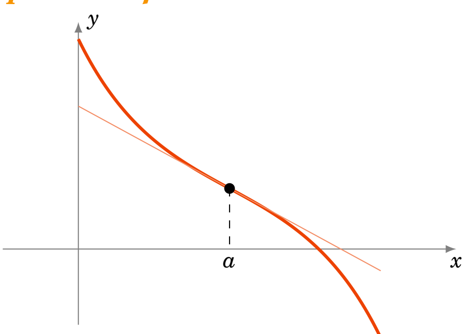
- Si le signe est positif alors la courbe est au-dessus de la tangente.



- Si le signe est négatif alors la courbe est en dessous de la tangente.



- Si le signe change (lorsque l'on passe de $x < a$ à $x > a$) alors la courbe traverse la tangente au point d'abscisse a. C'est un ***point d'inflexion***.

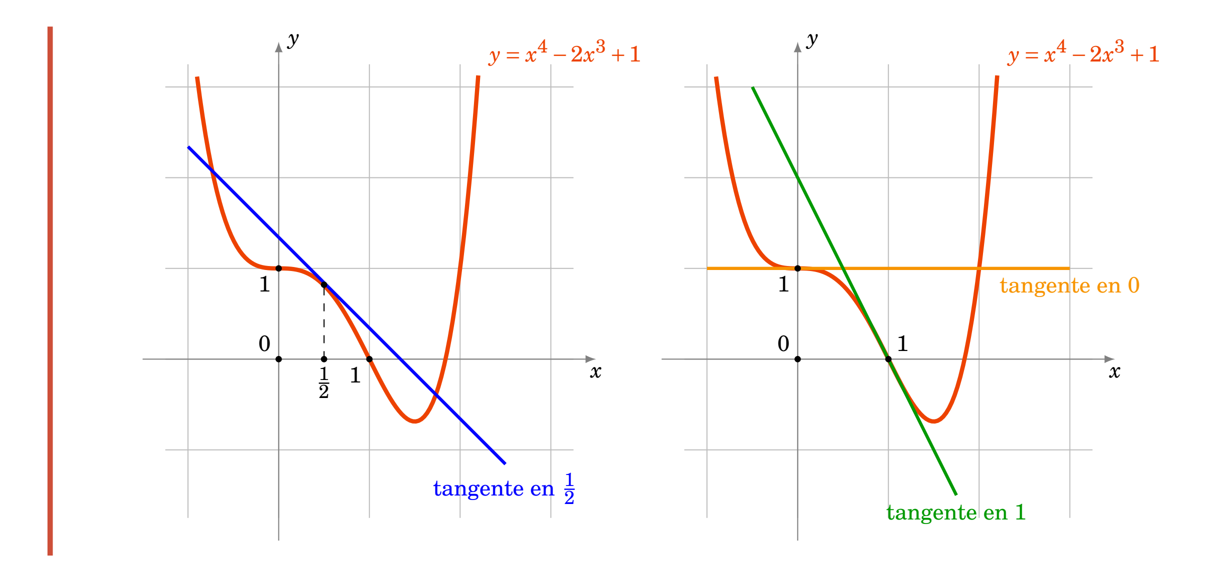


Comme le DL de f en a à l'ordre 2 s'écrit aussi $f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2}(x-a)^2 + (x-a)^2\varepsilon(x)$. Alors l'équation de la tangente est aussi $y = f(a) + f'(a)(x-a)$. Si en plus $f''(a) \neq 0$ alors $f(x) - y$ garde un signe constant autour de a. En conséquence si a est un point d'inflexion alors $f''(a) = 0$. (La réciproque est fausse.)

Exemple 141

Soit $f(x) = x^4 - 2x^3 + 1$.

1. Déterminons la tangente en $\frac{1}{2}$ du graphe de f et précisons la position du graphe par rapport à la tangente.
   On a $f'(x) = 4x^3 - 6x^2$, $f''(x) = 12x^2 - 12x$, donc $f''(\frac{1}{2}) = -3 \neq 0$ et $k = 2$.
   On en déduit le DL de f en $\frac{1}{2}$ par la formule de Taylor-Young : $f(x) = f(\frac{1}{2}) + f'(\frac{1}{2})(x - \frac{1}{2}) + \frac{f''(\frac{1}{2})}{2!}(x-\frac{1}{2})^2 + (x-\frac{1}{2})^2\varepsilon(x) = \frac{13}{16} - (x-\frac{1}{2}) - \frac{3}{2}(x-\frac{1}{2})^2 + (x-\frac{1}{2})^2\varepsilon(x)$.
   Donc la tangente en $\frac{1}{2}$ est $y = \frac{13}{16} - (x-\frac{1}{2})$ et le graphe de f est en dessous de la tangente car $f(x) - y = \big(-\frac{3}{2} + \varepsilon(x)\big)(x-\frac{1}{2})^2$ est négatif autour de $x = \frac{1}{2}$.
2. Déterminons les points d'inflexion.
   Les points d'inflexion sont à chercher parmi les solutions de $f''(x) = 0$. Donc parmi $x = 0$ et $x = 1$.
   - Le DL en 0 est $f(x) = 1 - 2x^3 + x^4$ (il s'agit juste d'écrire les monômes par degrés croissants !). L'équation de la tangente au point d'abscisse 0 est donc $y = 1$ (une tangente horizontale). Comme $-2x^3$ change de signe en 0 alors 0 est un point d'inflexion de f.
   - Le DL en 1 : on calcule $f(1)$, $f'(1)$, ... pour trouver le DL en 1 $f(x) = -2(x-1) + 2(x-1)^3 + (x-1)^4$. L'équation de la tangente au point d'abscisse 1 est donc $y = -2(x-1)$. Comme $2(x-1)^3$ change de signe en 1, 1 est aussi un point d'inflexion de f.



4.3. Développement limité en $+\infty$

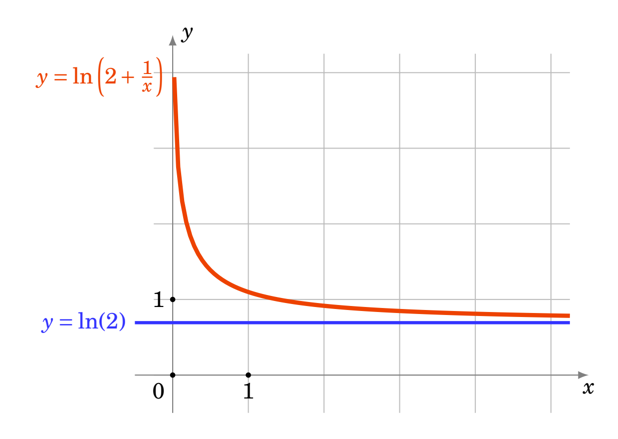
Soit f une fonction définie sur un intervalle $I =]x_0, +\infty[$. On dit que f admet un ***DL en*** $+\infty$ à l'ordre n s'il existe des réels $c_0, c_1, \ldots, c_n$ tels que

$$f(x) = c_0 + \frac{c_1}{x} + \cdots + \frac{c_n}{x^n} + \frac{1}{x^n}\varepsilon\left(\frac{1}{x}\right)$$

où $\varepsilon\left(\frac{1}{x}\right)$ tend vers 0 quand $x \to +\infty$.

Exemple 142

$f(x) = \ln\left(2 + \frac{1}{x}\right) = \ln 2 + \ln\left(1 + \frac{1}{2x}\right) = \ln 2 + \frac{1}{2x} - \frac{1}{8x^2} + \frac{1}{24x^3} + \cdots + (-1)^{n-1}\frac{1}{n2^n x^n} + \frac{1}{x^n}\varepsilon\left(\frac{1}{x}\right)$, où $\lim_{x\to\infty} \varepsilon\left(\frac{1}{x}\right) = 0$



Cela nous permet d'avoir une idée assez précise du comportement de f au voisinage de $+\infty$. Lorsque $x \to +\infty$ alors $f(x) \to \ln 2$. Et le second terme est $+\frac{1}{2}x$, donc est positif, cela signifie que la fonction $f(x)$ tend vers $\ln 2$ tout en restant au-dessus de $\ln 2$.

Remarque

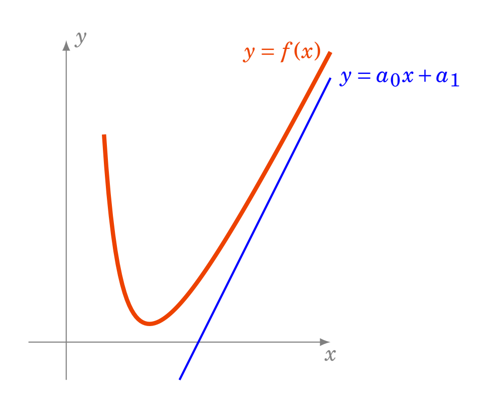
1. Un DL en $+\infty$ s'appelle aussi un développement asymptotique.
2. Dire que la fonction $x \mapsto f(x)$ admet un DL en $+\infty$ à l'ordre n est équivalent à dire que

la fonction $x \to f(\frac{1}{x})$ admet un DL en 0^+ à l'ordre n.

3. On peut définir de même ce qu'est un DL en $-\infty$.

Proposition 89

On suppose que la fonction $x \mapsto \frac{f(x)}{x}$ admet un DL en $+\infty$ (ou en $-\infty$) : $\frac{f(x)}{x} = a_0 + \frac{a_1}{x} + \frac{a_k}{x^k} + \frac{1}{x^k}\varepsilon(\frac{1}{x})$, où k est le plus petit entier $\geqslant 2$ tel que le coefficient de $\frac{1}{x^k}$ soit non nul. Alors $\lim_{x\to+\infty} f(x) - (a_0x + a_1) = 0$ (resp. $x \to -\infty$) : la droite $y = a_0x + a_1$ est une ***asymptote*** à la courbe de f en $+\infty$ (ou $-\infty$) et la position de la courbe par rapport à l'asymptote est donnée par le signe de $f(x) - y$, c'est-à-dire le signe de $\frac{a_k}{x^{k-1}}$.

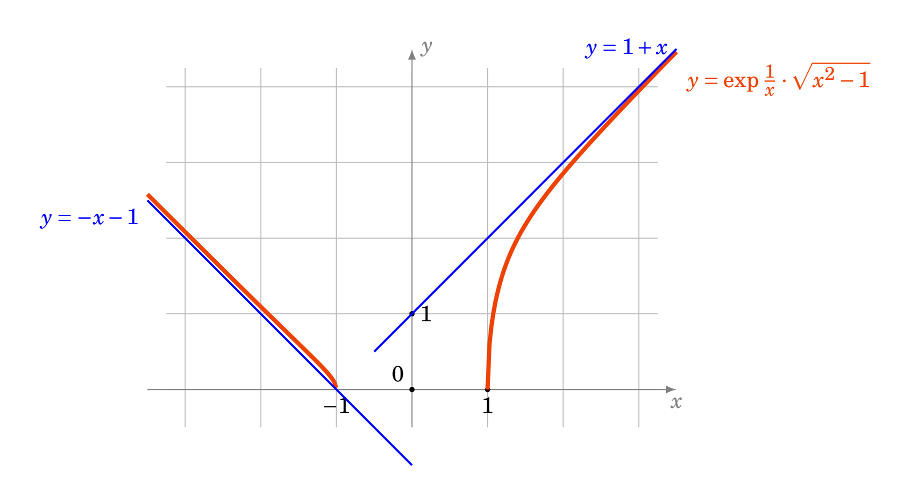


Démonstration

On a $\lim_{x\to+\infty}\big(f(x) - a_0x - a_1\big) = \lim_{x\to+\infty} \frac{a_k}{x^{k-1}} + \frac{1}{x^{k-1}}\varepsilon(\frac{1}{x}) = 0$. Donc $y = a_0x + a_1$ est une asymptote à la courbe de f. Ensuite on calcule la différence $f(x) - a_0x - a_1 = \frac{a_k}{x^{k-1}} + \frac{1}{x^{k-1}}\varepsilon(\frac{1}{x}) = \frac{a_k}{x^{k-1}}\big(1 + \frac{1}{a_k}\varepsilon(\frac{1}{x})\big)$.

Exemple 143

Asymptote de $f(x) = \exp\frac{1}{x} \cdot \sqrt{x^2 - 1}$.



1. En $+\infty$,

$$\begin{aligned}\frac{f(x)}{x} &= \exp\frac{1}{x}\cdot\frac{\sqrt{x^2-1}}{x} = \exp\frac{1}{x}\cdot\sqrt{1-\frac{1}{x^2}}\\ &= \left(1+\frac{1}{x}+\frac{1}{2x^2}+\frac{1}{6x^3}+\frac{1}{x^3}\varepsilon(\frac{1}{x})\right)\cdot\left(1-\frac{1}{2x^2}+\frac{1}{x^3}\varepsilon(\frac{1}{x})\right)\\ &= \cdots = 1+\frac{1}{x}-\frac{1}{3x^3}+\frac{1}{x^3}\varepsilon(\frac{1}{x})\end{aligned}$$

   Donc l'asymptote de f en $+\infty$ est $y = x+1$. Comme $f(x)-x-1 = -\frac{1}{3x^2}+\frac{1}{x^2}\varepsilon(\frac{1}{x})$ quand $x\to+\infty$, le graphe de f reste en dessous de l'asymptote.

2. En $-\infty$. $\frac{f(x)}{x} = \exp\frac{1}{x}\cdot\frac{\sqrt{x^2-1}}{x} = -\exp\frac{1}{x}\cdot\sqrt{1-\frac{1}{x^2}} = -1-\frac{1}{x}+\frac{1}{3x^3}+\frac{1}{x^3}\varepsilon(\frac{1}{x})$. Donc $y=-x-1$ est une asymptote de f en $-\infty$. On a $f(x)+x+1 = \frac{1}{3x^2}+\frac{1}{x^2}\varepsilon(\frac{1}{x})$ quand $x\to-\infty$; le graphe de f reste au-dessus de l'asymptote.

Mini-exercices

1. Calculer la limite de $\frac{\sin x - x}{x^3}$ lorsque x tend vers 0. Idem avec $\frac{\sqrt{1+x}-\operatorname{sh}\frac{x}{2}}{x^k}$ (pour $k = 1,2,3,\ldots$).
2. Calculer la limite de $\frac{\sqrt{x}-1}{\ln x}$ lorsque x tend vers 1. Idem pour $\left(\frac{1-x}{1+x}\right)^{\frac{1}{x}}$, puis $\frac{1}{\tan^2 x}-\frac{1}{x^2}$ lorsque x tend vers 0.
3. Soit $f(x) = \exp x + \sin x$. Calculer l'équation de la tangente en $x = 0$ et la position du graphe. Idem avec $g(x) = \operatorname{sh} x$.
4. Calculer le DL en $+\infty$ à l'ordre 5 de $\frac{x}{x^2-1}$. Idem à l'ordre 2 pour $\left(1+\frac{1}{x}\right)^x$.
5. Soit $f(x) = \sqrt{\frac{x^3+1}{x+1}}$. Déterminer l'asymptote en $+\infty$ et la position du graphe par rapport à cette asymptote.

Auteurs

Rédaction : Arnaud Bodin
Basé sur des cours de Guoting Chen et Marc Bourdon
Relecture : Pascal Romon
Dessins : Benjamin Boutin



14 Groupes

Vidéo ■ partie 1. Définition
Vidéo ■ partie 2. Sous-groupes
Vidéo ■ partie 3. Morphismes de groupes
Vidéo ■ partie 4. Le groupe $\mathbb{Z}/n\mathbb{Z}$
Vidéo ■ partie 5. Le groupe des permutations

Motivation

Évariste Galois a tout juste vingt ans lorsqu'il meurt dans un duel. Il restera pourtant comme l'un des plus grands mathématiciens de son temps pour avoir introduit la notion de groupe, alors qu'il avait à peine dix-sept ans.
Vous savez résoudre les équations de degré 2 du type $ax^2+bx+c=0$. Les solutions s'expriment en fonction de a,b,c et de la fonction racine carrée $\sqrt{\ }$. Pour les équations de degré 3, $ax^3+bx^2+cx+d=0$, il existe aussi des formules. Par exemple une solution de $x^3+3x+1=0$ est $x_0=\sqrt[3]{\frac{\sqrt{5}-1}{2}}-\sqrt[3]{\frac{\sqrt{5}+1}{2}}$. De telles formules existent aussi pour les équations de degré 4.
Un préoccupation majeure au début du XIXe siècle était de savoir s'il existait des formules similaires pour les équations de degré 5 ou plus. La réponse fut apportée par Galois et Abel : non il n'existe pas en général une telle formule. Galois parvient même à dire pour quels polynômes c'est possible et pour lesquels ce ne l'est pas. Il introduit pour sa démonstration la notion de groupe.

Les groupes sont à la base d'autres notions mathématiques comme les anneaux, les corps, les matrices, les espaces vectoriels,... Mais vous les retrouvez aussi en arithmétique, en géométrie, en cryptographie !

Nous allons introduire dans ce chapitre la notion de groupe, puis celle de sous-groupe. On étudiera ensuite les applications entre deux groupes : les morphismes de groupes. Finalement nous détaillerons deux groupes importants : le groupe $\mathbb{Z}/n\mathbb{Z}$ et le groupe des permutations $\mathcal{S}_n$.

1. Groupe

1.1. Définition

Définition 68

Un ***groupe*** $(G,\star)$ est un ensemble G auquel est associé une opération $\star$ (la ***loi de composition***) vérifiant les quatre propriétés suivantes :

1. pour tout $x,y\in G$, $\quad x\star y\in G \quad$ ($\star$ est une ***loi de composition interne***)
2. pour tout $x,y,z\in G$, $\quad (x\star y)\star z = x\star(y\star z) \quad$ (la loi est ***associative***)
3. il existe $e\in G$ tel que $\quad \forall x\in G,\ x\star e = x$ et $e\star x = x \quad$ (e est l'***élément neutre***)
4. pour tout $x\in G$ il existe $x'\in G$ tel que $\quad x\star x' = x'\star x = e \quad$ (x' est l'***inverse*** de x et est noté x^{-1})

Si de plus l'opération vérifie

$$\text{pour tous } x,y\in G,\qquad x\star y = y\star x,$$

on dit que G est un groupe ***commutatif*** (ou ***abélien***).

Remarque

- L'élément neutre e est unique. En effet si e' vérifie aussi le point (3), alors on a $e'\star e = e$ (car e est élément neutre) et $e'\star e = e'$ (car e' aussi). Donc $e = e'$. Remarquez aussi que l'inverse de l'élément neutre est lui-même. S'il y a plusieurs groupes, on pourra noter e_G pour l'élément neutre du groupe G.
- Un élément $x\in G$ ne possède qu'un seul inverse. En effet si x' et x'' vérifient tous les deux le point (4) alors on a $x\star x'' = e$ donc $x'\star(x\star x'') = x'\star e$. Par l'associativité (2) et la propriété de l'élément neutre (3) alors $(x'\star x)\star x'' = x'$. Mais $x'\star x = e$ donc $e\star x'' = x'$ et ainsi $x'' = x'$.

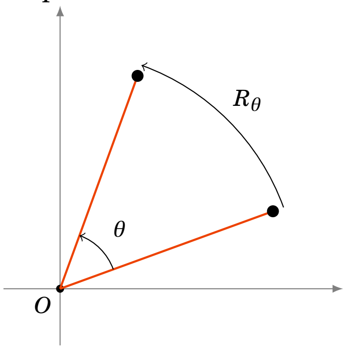
1.2. Exemples

Voici des ensembles et des opérations bien connus qui ont une structure de groupe.

- $(\mathbb{R}^*,\times)$ est un groupe commutatif, $\times$ est la multiplication habituelle. Vérifions chacune des propriétés :
  1. Si $x,y\in\mathbb{R}^*$ alors $x\times y\in\mathbb{R}^*$.
  2. Pour tout $x,y,z\in\mathbb{R}^*$ alors $x\times(y\times z) = (x\times y)\times z$, c'est l'associativité de la multiplication des nombres réels.
  3. 1 est l'élément neutre pour la multiplication, en effet $1\times x = x$ et $x\times 1 = x$, ceci quelque soit $x\in\mathbb{R}^*$.
  4. L'inverse d'un élément $x\in\mathbb{R}^*$ est $x' = \frac{1}{x}$ (car $x\times\frac{1}{x}$ est bien égal à l'élément neutre 1). L'inverse de x est donc $x^{-1} = \frac{1}{x}$. Notons au passage que nous avions exclu 0 de notre groupe, car il n'a pas d'inverse.
     Ces propriétés font de $(\mathbb{R}^*,\times)$ un groupe.
  5. Enfin $x\times y = y\times x$, c'est la commutativité de la multiplication des réels.
- $(\mathbb{Q}^*,\times)$, $(\mathbb{C}^*,\times)$ sont des groupes commutatifs.
- $(\mathbb{Z},+)$ est un groupe commutatif. Ici $+$ est l'addition habituelle.
  1. Si $x,y\in\mathbb{Z}$ alors $x+y\in\mathbb{Z}$.

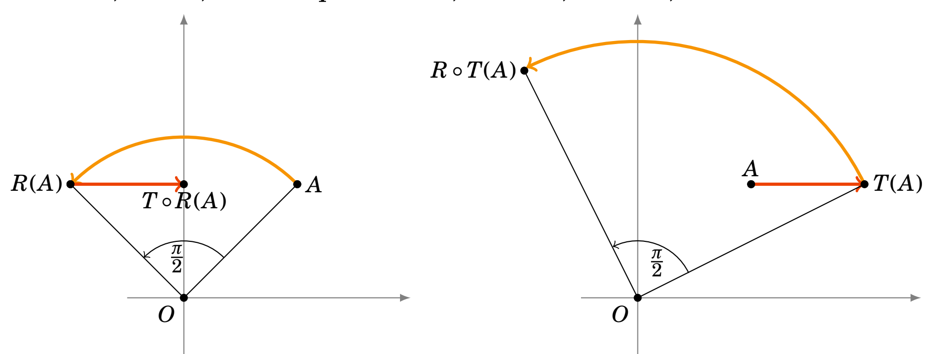
2. Pour tout $x, y, z \in \mathbb{Z}$ alors $x + (y + z) = (x + y) + z$.
3. 0 est l'élément neutre pour l'addition, en effet $0 + x = x$ et $x + 0 = x$, ceci quelque soit $x \in \mathbb{Z}$.
4. L'inverse d'un élément $x \in \mathbb{Z}$ est $x' = -x$ car $x + (-x) = 0$ est bien l'élément neutre 0. Quand la loi de groupe est + l'inverse s'appelle plus couramment l'***opposé***.
5. Enfin $x + y = y + x$, et donc $(\mathbb{Z}, +)$ est un groupe commutatif.

- $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes commutatifs.
- Soit $\mathscr{R}$ l'ensemble des rotations du plan dont le centre est à l'origine O.



Alors pour deux rotations R_θ et $R_{\theta'}$ la composée $R_\theta \circ R_{\theta'}$ est encore une rotation de centre l'origine et d'angle $\theta + \theta'$. Ici $\circ$ est la composition. Ainsi $(\mathscr{R}, \circ)$ forme un groupe (qui est même commutatif). Pour cette loi l'élément neutre est la rotation d'angle 0 : c'est l'identité du plan. L'inverse d'une rotation d'angle θ est la rotation d'angle $-\theta$.

- Si $\mathscr{I}$ désigne l'ensemble des isométries du plan (ce sont les translations, rotations, réflexions et leurs composées) alors $(\mathscr{I}, \circ)$ est un groupe. Ce groupe n'est pas un groupe commutatif. En effet, identifions le plan à $\mathbb{R}^2$ et soit par exemple R la rotation de centre $O = (0,0)$ et d'angle $\frac{\pi}{2}$ et T la translation de vecteur $(1,0)$. Alors les isométries $T \circ R$ et $R \circ T$ sont des applications distinctes. Par exemple les images du point $A = (1,1)$ par ces applications sont distinctes : $T \circ R(1,1) = T(-1,1) = (0,1)$ alors que $R \circ T(1,1) = R(2,1) = (-1,2)$.



Voici deux exemples qui **ne sont pas** des groupes :

- $(\mathbb{Z}^*, \times)$ n'est pas un groupe. Car si 2 avait un inverse (pour la multiplication $\times$) ce serait $\frac{1}{2}$ qui n'est pas un entier.
- $(\mathbb{N}, +)$ n'est pas un groupe. En effet l'inverse de 3 (pour l'addition +) devrait être -3 mais $-3 \notin \mathbb{N}$.

Nous étudierons dans les sections 4 et 5 deux autres groupes très importants : les groupes cycliques $(\mathbb{Z}/n\mathbb{Z}, +)$ et les groupes de permutations $(\mathscr{S}_n, \circ)$.

1.3. Puissance

Revenons à un groupe $(G, \star)$. Pour $x \in G$ nous noterons $x \star x$ par x^2 et $x \star x \star x$ par x^3. Plus généralement nous noterons :

- $x^n = \underbrace{x \star x \star \cdots \star x}_{n \text{ fois}}$,
- $x^0 = e$,
- $x^{-n} = \underbrace{x^{-1} \star \cdots \star x^{-1}}_{n \text{ fois}}$.

Rappelez-vous que x^{-1} désigne l'inverse de x dans le groupe.

Les règles de calcul sont les mêmes que pour les puissances des nombres réels. Pour $x, y \in G$ et $m, n \in \mathbb{Z}$ nous avons :

- $x^m \star x^n = x^{m+n}$,
- $(x^m)^n = x^{mn}$,
- $(x \star y)^{-1} = y^{-1} \star x^{-1}$, attention à l'ordre !
- **Si** $(G, \star)$ est **commutatif** alors $(x \star y)^n = x^n \star y^n$.

1.4. Exemple des matrices 2×2

Une ***matrice*** 2×2 est un tableau de 4 nombres (pour nous des réels) notée ainsi :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Nous allons définir l'opération ***produit*** noté $\times$ de deux matrices $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ et $M' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$:

$$M \times M' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Voici comment présenter les calculs, on place M à gauche, M' au dessus de ce qui va être le résultat. On calcule un par un, chacun des termes de $M \times M'$.
Pour le premier terme on prend la colonne située au dessus et la ligne située à gauche : on effectue les produits $a \times a'$ et $b \times c'$ qu'on additionne pour obtenir le premier terme du résultat. Même chose avec le second terme : on prend la colonne située au dessus, la ligne située à gauche, on fait les produit, on additionne : $ab' + bd'$. Idem pour les deux autres termes.

$$\begin{array}{cc} & \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix} \end{array}$$

Par exemple si $M = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$ et $M' = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$ alors voici comment poser les calculs ($M \times M'$ à gauche, $M' \times M$ à droite)

$$\begin{array}{cc} & \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} & \begin{pmatrix} 3 & 1 \\ -2 & -1 \end{pmatrix} \end{array} \qquad \begin{array}{cc} & \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \end{array}$$

alors $M \times M' = \left(\begin{smallmatrix} 3 & 1 \\ -2 & -1 \end{smallmatrix}\right)$ et $M' \times M = \left(\begin{smallmatrix} 1 & 1 \\ 2 & 1 \end{smallmatrix}\right)$. Remarquez qu'en général $M \times M' \neq M' \times M$.

Le ***déterminant*** d'une matrice $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est par définition le nombre réel

$$\det M = ad - bc.$$

Proposition 90

L'ensemble des matrices 2×2 ayant un déterminant non nul, muni de la multiplication des matrices $\times$, forme un groupe non-commutatif.

Ce groupe est noté $(\mathcal{G}\ell_2, \times)$.

Nous aurons besoin d'un résultat préliminaire :

Lemme 7

$\det(M \times M') = \det M \cdot \det M'$.

Pour la preuve, il suffit de vérifier le calcul : $(aa' + bc')(cb' + dd') - (ab' + bd')(ca' + dc') = (ad - bc)(a'd' - b'c')$.
Revenons à la preuve de la proposition.

Démonstration

1. Vérifions la loi de composition interne. Si M, M' sont des matrices 2×2 alors $M \times M'$ aussi. Maintenant si M et M' sont de déterminants non nuls alors $\det(M \times M') = \det M \cdot \det M'$ est aussi non nul. Donc si $M, M' \in \mathcal{G}\ell_2$ alors $M \times M' \in \mathcal{G}\ell_2$.
2. Pour vérifier que la loi est associative, c'est un peu fastidieux. Pour trois matrices M, M', M'' quelconques il faut montrer $(M \times M') \times M'' = M \times (M' \times M'')$. Faites-le pour vérifier que vous maîtrisez le produit de matrices.
3. Existence de l'élément neutre. La ***matrice identité*** $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ est l'élément neutre pour la multiplication des matrices : en effet $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \times \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.
4. Existence de l'inverse. Soit $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ une matrice de déterminant non nul alors $M^{-1} = \frac{1}{ad-bc} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ est l'inverse de M : vérifiez que $M \times M^{-1} = I$ et que $M^{-1} \times M = I$.
5. Enfin nous avons déjà vu que cette multiplication n'est pas commutative.

Mini-exercices

1. Montrer que $(\mathbb{R}_+^*, \times)$ est un groupe commutatif.
2. Soit $f_{a,b} : \mathbb{R} \to \mathbb{R}$ la fonction définie par $x \mapsto ax + b$. Montrer que l'ensemble $\mathcal{F} = \{f_{a,b} \mid a \in \mathbb{R}^*, b \in \mathbb{R}\}$ muni de la composition «$\circ$» est un groupe non commutatif.
3. (Plus dur) Soit $G =]-1, 1[$. Pour $x, y \in G$ on définit $x \star y = \frac{x+y}{1+xy}$. Montrer que $(G, \star)$ forme un groupe en (a) montrant que $\star$ est une loi de composition interne : $x \star y \in G$; (b) montrant que la loi est associative ; (c) montrant que 0 est élément neutre ; (d) trouvant l'inverse de x.

Soit $(G, \star)$ est un groupe quelconque, x, y, z sont des éléments de G.

4. Montrer que si $x \star y = x \star z$ alors $y = z$.
5. Que vaut $(x^{-1})^{-1}$?
6. Si $x^n = e$, quel est l'inverse de x ?

Matrices :

7. Soient $M_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $M_2 = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$, $M_3 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. Vérifier que $M_1 \times (M_2 \times M_3) = (M_1 \times M_2) \times M_3$.
8. Calculer $(M_1 \times M_2)^2$ et $M_1^2 \times M_2^2$. (Rappel : $M^2 = M \times M$)
9. Calculer les déterminants des M_i ainsi que leur inverse.
10. Montrer que l'ensemble des matrices 2×2 muni de l'addition + définie par $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$ forme un groupe commutatif.

2. Sous-groupes

Montrer qu'un ensemble est un groupe à partir de la définition peut être assez long. Il existe une autre technique, c'est de montrer qu'un sous-ensemble d'un groupe est lui-même un groupe : c'est la notion de sous-groupe.

2.1. Définition

Soit $(G, \star)$ un groupe.

Définition 69

Une partie $H \subset G$ est un ***sous-groupe*** de G si :
- $e \in H$,
- pour tout $x, y \in H$, on a $x \star y \in H$,
- pour tout $x \in H$, on a $x^{-1} \in H$.

Notez qu'un sous-groupe H est aussi un groupe $(H, \star)$ avec la loi induite par celle de G.
Par exemple si $x \in H$ alors, pour tout $n \in \mathbb{Z}$, nous avons $x^n \in H$.

Remarque

Un critère pratique et plus rapide pour prouver que H est un sous-groupe de G est :
- H contient au moins un élément
- pour tout $x, y \in H$, $x \star y^{-1} \in H$.

2.2. Exemples

- $(\mathbb{R}_+^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$. En effet :
  - $1 \in \mathbb{R}_+^*$,
  - si $x, y \in \mathbb{R}_+^*$ alors $x \times y \in \mathbb{R}_+^*$,
  - si $x \in \mathbb{R}_+^*$ alors $x^{-1} = \frac{1}{x} \in \mathbb{R}_+^*$.
- $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$, où $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.
- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.
- $\{e\}$ et G sont les ***sous-groupes triviaux*** du groupe G.
- L'ensemble $\mathscr{R}$ des rotations du plan dont le centre est à l'origine est un sous-groupe du groupe des isométries $\mathscr{I}$.
- L'ensemble des matrices diagonales $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ avec $a \neq 0$ et $d \neq 0$ est un sous-groupe de $(\mathscr{GL}_2, \times)$.

2.3. Sous-groupes de $\mathbb{Z}$

Proposition 91

Les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{Z}$.

L'ensemble $n\mathbb{Z}$ désigne l'ensemble des multiples de n :

$$n\mathbb{Z} = \Big\{ k \cdot n \mid k \in \mathbb{Z} \Big\}.$$

Par exemple :
- $2\mathbb{Z} = \{\ldots,-4,-2,0,+2,+4,+6,\ldots\}$ est l'ensemble des entiers pairs,
- $7\mathbb{Z} = \{\ldots,-14,-7,0,+7,+14,+21,\ldots\}$ est l'ensemble des multiples de 7.

Démonstration

Fixons $n \in \mathbb{Z}$. L'ensemble $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$, en effet :
- $n\mathbb{Z} \subset \mathbb{Z}$,
- l'élément neutre 0 appartient à $n\mathbb{Z}$,
- pour $x = kn$ et $y = k'n$ des éléments de $n\mathbb{Z}$ alors $x + y = (k + k')n$ est aussi un élément de $n\mathbb{Z}$,
- enfin si $x = kn$ est un élément de $n\mathbb{Z}$ alors $-x = (-k)n$ est aussi un élément de $n\mathbb{Z}$.

Réciproquement soit H un sous-groupe de $(\mathbb{Z},+)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$ et c'est fini. Sinon H contient au moins un élément non-nul et positif (puisque tout élément est accompagné de son opposé) et notons

$$n = \min\big\{ h > 0 \mid h \in H \big\}.$$

Alors $n > 0$. Comme $n \in H$ alors $-n \in H$, $2n = n+n \in H$, et plus généralement pour $k \in \mathbb{Z}$ alors $kn \in H$. Ainsi $n\mathbb{Z} \subset H$. Nous allons maintenant montrer l'inclusion inverse. Soit $h \in H$. Écrivons la division euclidienne :

$$h = kn + r, \qquad \text{avec } k,r \in \mathbb{Z} \text{ et } 0 \leqslant r < n.$$

Mais $h \in H$ et $kn \in H$ donc $r = h - kn \in H$. Nous avons un entier $r \geqslant 0$ qui est un élément de H et strictement plus petit que n. Par la définition de n, nécessairement $r = 0$. Autrement dit $h = kn$ et donc $h \in n\mathbb{Z}$. Conclusion $H = n\mathbb{Z}$.

2.4. Sous-groupes engendrés

Soit $(G,\star)$ un groupe et $E \subset G$ un sous-ensemble de G. Le ***sous-groupe engendré*** par E est le plus petit sous-groupe de G contenant E.
Par exemple si $E = \{2\}$ et le groupe est $(\mathbb{R}^*,\times)$, le sous-groupe engendré par E est $H = \{2^n \mid n \in \mathbb{Z}\}$. Pour le prouver : il faut montrer que H est un sous-groupe, que $2 \in H$, et que si H' est un autre sous-groupe contenant 2 alors $H \subset H'$.
Autre exemple avec le groupe $(\mathbb{Z},+)$: si $E_1 = \{2\}$ alors le sous-groupe engendré par E_1 est $H_1 = 2\mathbb{Z}$. Si $E_2 = \{8,12\}$ alors $H_2 = 4\mathbb{Z}$ et plus généralement si $E = \{a,b\}$ alors $H = n\mathbb{Z}$ où $n = \text{pgcd}(a,b)$.

2.5. Mini-exercices

1. Montrer que $\{2^n \mid n \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{R}^*,\times)$.
2. Montrer que si H et H' sont deux sous-groupes de $(G,\star)$ alors $H \cap H'$ est aussi un sous-groupe.
3. Montrer que $5\mathbb{Z} \cup 8\mathbb{Z}$ n'est *pas* un sous-groupe de $(\mathbb{Z},+)$.
4. Montrer que l'ensemble des matrices 2×2 de déterminant 1 ayant leurs coefficients dans $\mathbb{Z}$ est un sous-groupe de $(\mathscr{G}\ell_2,\times)$.
5. Trouver le sous-groupe de $(\mathbb{Z},+)$ engendré par $\{-12,8,20\}$.

3. Morphismes de groupes

3.1. Définition

Définition 70

Soient $(G,\star)$ et $(G',\diamond)$ deux groupes. Une application $f : G \longrightarrow G'$ est un ***morphisme de groupes*** si :

$$\text{pour tout } x, x' \in G \qquad f(x \star x') = f(x) \diamond f(x')$$

L'exemple que vous connaissez déjà est le suivant : soit G le groupe $(\mathbb{R},+)$ et G' le groupe $(\mathbb{R}_+^*, \times)$. Soit $f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ l'application exponentielle définie par $f(x) = \exp(x)$. Nous avons bien

$$f(x+x') = \exp(x+x') = \exp(x) \times \exp(x') = f(x) \times f(x').$$

Et donc f est bien un morphisme de groupes.

3.2. Propriétés

Proposition 92

Soit $f : G \longrightarrow G'$ un morphisme de groupes alors :

- $f(e_G) = e_{G'}$,
- pour tout $x \in G$, $f(x^{-1}) = \big(f(x)\big)^{-1}$.

Il faut faire attention où «habitent» les objets : e_G est l'élément neutre de G, $e_{G'}$ celui de G'. Il n'y a pas de raison qu'ils soient égaux (ils ne sont même pas dans le même ensemble). Aussi x^{-1} est l'inverse de x dans G, alors que $\big(f(x)\big)^{-1}$ est l'inverse de $f(x)$ mais dans G'.
Reprenons l'exemple de la fonction $f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ définie par $f(x) = \exp(x)$. Nous avons bien $f(0) = 1$: l'élément neutre de $(\mathbb{R},+)$ a pour image l'élément neutre de $(\mathbb{R}_+^*, \times)$. Pour $x \in \mathbb{R}$ son inverse dans $(\mathbb{R},+)$ est ici son opposé $-x$, alors $f(-x) = \exp(-x) = \frac{1}{\exp(x)} = \frac{1}{f(x)}$ est bien l'inverse (dans $(\mathbb{R}_+^*, \times)$) de $f(x)$.

Démonstration

- $f(e_G) = f(e_G \star e_G) = f(e_G) \diamond f(e_G)$, en multipliant (à droite par exemple) par $f(e_G)^{-1}$ on obtient $e_{G'} = f(e_G)$.
- Soit $x \in G$ alors $x \star x^{-1} = e_G$ donc $f(x \star x^{-1}) = f(e_G)$. Cela entraîne $f(x) \diamond f(x^{-1}) = e_{G'}$, en composant à gauche par $\big(f(x)\big)^{-1}$, nous obtenons $f(x^{-1}) = \big(f(x)\big)^{-1}$.

Proposition 93

- Soient deux morphismes de groupes $f : G \longrightarrow G'$ et $g : G' \longrightarrow G''$. Alors $g \circ f : G \longrightarrow G''$ est un morphisme de groupes.
- Si $f : G \longrightarrow G'$ est un morphisme bijectif alors $f^{-1} : G' \longrightarrow G$ est aussi un morphisme de groupes.

Démonstration

La première partie est facile. Montrons la deuxième : Soit $y, y' \in G'$. Comme f est bijective, il existe $x, x' \in G$ tels que $f(x) = y$ et $f(x') = y'$. Alors $f^{-1}(y \diamond y') = f^{-1}\big(f(x) \diamond f(x')\big) = f^{-1}\big(f(x \star x')\big) = x \star x' = f^{-1}(y) \star f^{-1}(y')$. Et donc f^{-1} est un morphisme de G' vers G.

Définition 71

Un morphisme bijectif est un ***isomorphisme***. Deux groupes G, G' sont ***isomorphes*** s'il existe un morphisme bijectif $f : G \longrightarrow G'$.

Continuons notre exemple $f(x) = \exp(x)$, $f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ est une application bijective. Sa bijection réciproque $f^{-1} : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ est définie par $f^{-1}(x) = \ln(x)$. Par la proposition 93 nous savons que f^{-1} est aussi un morphisme (de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$) donc $f^{-1}(x \times x') = f^{-1}(x) + f^{-1}(x')$. Ce qui s'exprime ici par la formule bien connue :

$$\ln(x \times x') = \ln(x) + \ln(x').$$

Ainsi f est un isomorphisme et les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes.

3.3. Noyau et image

Soit $f : G \longrightarrow G'$ un morphisme de groupes. Nous définissons deux sous-ensembles importants qui vont être des sous-groupes.

Définition 72

Le ***noyau*** de f est

$$\boxed{\operatorname{Ker} f = \big\{x \in G \mid f(x) = e_{G'}\big\}}$$

C'est donc un sous-ensemble de G. En terme d'image réciproque nous avons par définition $\operatorname{Ker} f = f^{-1}\big(\{e_{G'}\}\big)$. (Attention, la notation f^{-1} ici désigne l'image réciproque, et ne signifie pas que f est bijective.) Le noyau est donc l'ensemble des éléments de G qui s'envoient par f sur l'élément neutre de G'.

Définition 73

L'***image*** de f est

$$\boxed{\operatorname{Im} f = \big\{f(x) \mid x \in G\big\}}$$

C'est donc un sous-ensemble de G' et en terme d'image directe nous avons $\operatorname{Im} f = f(G)$. Ce sont les éléments de G' qui ont (au moins) un antécédent par f.

Proposition 94

Soit $f : G \longrightarrow G'$ un morphisme de groupes.

1. $\operatorname{Ker} f$ est un sous-groupe de G.
2. $\operatorname{Im} f$ est un sous-groupe de G'.
3. f est injectif si et seulement si $\operatorname{Ker} f = \{e_G\}$.
4. f est surjectif si et seulement si $\operatorname{Im} f = G'$.

Démonstration

1. Montrons que le noyau est un sous-groupe de G.
   (a) $f(e_G) = e_{G'}$ donc $e_G \in \operatorname{Ker} f$.
   (b) Soient $x, x' \in \operatorname{Ker} f$. Alors $f(x \star x') = f(x) \diamond f(x') = e_{G'} \diamond e_{G'} = e_{G'}$ et donc $x \star x' \in \operatorname{Ker} f$.
   (c) Soit $x \in \operatorname{Ker} f$. Alors $f(x^{-1}) = f(x)^{-1} = e_{G'}^{-1} = e_{G'}$. Et donc $x^{-1} \in \operatorname{Ker} f$.
2. Montrons que l'image est un sous-groupe de G'.
   (a) $f(e_G) = e_{G'}$ donc $e_{G'} \in \operatorname{Im} f$.
   (b) Soient $y, y' \in \operatorname{Im} f$. Il existe alors $x, x' \in G$ tels que $f(x) = y$, $f(x') = y'$. Alors $y \diamond y' = f(x) \diamond f(x') = f(x \star x') \in \operatorname{Im} f$.
   (c) Soit $y \in \operatorname{Im} f$ et $x \in G$ tel que $y = f(x)$. Alors $y^{-1} = f(x)^{-1} = f(x^{-1}) \in \operatorname{Im} f$.
3. Supposons f injective. Soit $x \in \operatorname{Ker} f$, alors $f(x) = e_{G'}$ donc $f(x) = f(e_G)$ et comme f est injective alors $x = e_G$. Donc $\operatorname{Ker} f = \{e_G\}$. Réciproquement supposons $\operatorname{Ker} f = \{e_G\}$. Soient $x, x' \in G$ tels que $f(x) = f(x')$ donc $f(x) \diamond \left(f(x')\right)^{-1} = e_{G'}$, d'où $f(x) \diamond f(x'^{-1}) = e_{G'}$ et donc $f(x \star x'^{-1}) = e_{G'}$. Ceci implique que $x \star x'^{-1} \in \operatorname{Ker} f$. Comme $\operatorname{Ker} f = \{e_G\}$ alors $x \star x'^{-1} = e_G$ et donc $x = x'$. Ainsi f est injective.
4. C'est clair !

3.4. Exemples

Exemple 144

1. Soit $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ définie par $f(k) = 3k$. $(\mathbb{Z}, +)$ est considéré comme ensemble de départ et d'arrivée de l'application Alors f est un morphisme du groupe $(\mathbb{Z}, +)$ dans lui-même car $f(k + k') = 3(k + k') = 3k + 3k' = f(k) + f(k')$. Calculons le noyau : $\operatorname{Ker} f = \{k \in \mathbb{Z} \mid f(k) = 0\}$. Mais si $f(k) = 0$ alors $3k = 0$ donc $k = 0$. Ainsi $\operatorname{Ker} f = \{0\}$ est réduit à l'élément neutre et donc f est injective. Calculons maintenant l'image $\operatorname{Im} f = \{f(k) \mid k \in \mathbb{Z}\} = \{3k \mid k \in \mathbb{Z}\} = 3\mathbb{Z}$. Nous retrouvons que $3\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.

   Plus généralement si l'on fixe $n \in \mathbb{Z}$ et que f est définie par $f(k) = k \cdot n$ alors $\operatorname{Ker} f = \{0\}$ et $\operatorname{Im} f = n\mathbb{Z}$.
2. Soient les groupes $(\mathbb{R}, +)$ et $(\mathbb{U}, \times)$ (où $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$) et f l'application $f : \mathbb{R} \longrightarrow \mathbb{U}$ définie par $f(t) = e^{it}$. Montrons que f est un morphisme : $f(t + t') = e^{\mathrm{i}(t+t')} = e^{\mathrm{i}t} \times e^{\mathrm{i}t'} = f(t) \times f(t')$. Calculons le noyau $\operatorname{Ker} f = \{t \in \mathbb{R} \mid f(t) = 1\}$. Mais si $f(t) = 1$ alors $e^{\mathrm{i}t} = 1$ donc $t = 0 \pmod{2\pi}$. D'où $\operatorname{Ker} f = \{2k\pi \mid k \in \mathbb{Z}\} = 2\pi\mathbb{Z}$. Ainsi f n'est pas injective. L'image de f est $\mathbb{U}$ car tout nombre complexe de module 1 s'écrit sous la forme $f(t) = e^{\mathrm{i}t}$.
3. Soient les groupes $(\mathscr{GL}_2, \times)$ et $(\mathbb{R}^*, \times)$ et $f : \mathscr{GL}_2 \longrightarrow \mathbb{R}^*$ définie par $f(M) = \det M$. Alors la formule vue plus haut (lemme 7) $\det(M \times M') = \det M \times \det M'$ implique que f est un morphisme de groupes. Ce morphisme est surjectif, car si $t \in \mathbb{R}^*$ alors $\det\left(\begin{smallmatrix} 1 & 0 \\ 0 & t \end{smallmatrix}\right) = t$. Ce morphisme n'est pas injectif car par exemple $\det\left(\begin{smallmatrix} 1 & 0 \\ 0 & t \end{smallmatrix}\right) = \det\left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Attention : ne pas confondre les différentes notations avec des puissances -1 : x^{-1}, f^{-1}, $f^{-1}\left(\{e_{G'}\}\right)$:

- x^{-1} désigne l'inverse de x dans un groupe $(G, \star)$. Cette notation est cohérente avec la notation usuelle si le groupe est $(\mathbb{R}^*, \times)$ alors $x^{-1} = \frac{1}{x}$.
- Pour une application bijective f^{-1} désigne la bijection réciproque.
- Pour une application quelconque $f : E \longrightarrow F$, l'image réciproque d'une partie $B \subset F$ est $f^{-1}(B) = \{x \in E \mid f(x) = B\}$, c'est une partie de E. Pour un morphisme f, $\operatorname{Ker} f = f^{-1}\left(\{e_{G'}\}\right)$ est

donc l'ensemble des $x \in G$ tels que leur image par f soit $e_{G'}$. Le noyau est défini même si f n'est pas bijective.

Mini-exercices

1. Soit $f : (\mathbb{Z},+) \longrightarrow (\mathbb{Q}^*,\times)$ défini par $f(n) = 2^n$. Montrer que f est un morphisme de groupes. Déterminer le noyau de f. f est-elle injective ? surjective ?
2. Mêmes questions pour $f : (\mathbb{R},+) \longrightarrow (\mathscr{R},\circ)$, qui à un réel θ associe la rotation d'angle θ de centre l'origine.
3. Soit $(G,\star)$ un groupe et $f : G \longrightarrow G$ l'application définie par $f(x) = x^2$. (Rappel : $x^2 = x \star x$.) Montrer que si $(G,\star)$ est commutatif alors f est un morphisme. Montrer ensuite la réciproque.
4. Montrer qu'il n'existe pas de morphisme $f : (\mathbb{Z},+) \to (\mathbb{Z},+)$ tel que $f(2) = 3$.
5. Montrer que $f, g : (\mathbb{R}^*,\times) \to (\mathbb{R}^*,\times)$ défini par $f(x) = x^2$, $g(x) = x^3$ sont des morphismes de groupes. Calculer leurs images et leurs noyaux respectives.

4. Le groupe $\mathbb{Z}/n\mathbb{Z}$

4.1. L'ensemble et le groupe $\mathbb{Z}/n\mathbb{Z}$

Fixons $n \geqslant 1$. Rappelons que $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}$$

où $\overline{p}$ désigne la classe d'équivalence de p modulo n.
Autrement dit

$$\boxed{\overline{p} = \overline{q} \iff p \equiv q \pmod n}$$

ou encore $\overline{p} = \overline{q} \iff \exists k \in \mathbb{Z} \quad p = q + kn$.
On définit une ***addition*** sur $\mathbb{Z}/n\mathbb{Z}$ par :

$$\boxed{\overline{p} + \overline{q} = \overline{p+q}}$$

Par exemple dans $\mathbb{Z}/60\mathbb{Z}$, on a $\overline{31} + \overline{46} = \overline{31+46} = \overline{77} = \overline{17}$.

Nous devons montrer que cette addition est bien définie : si $\overline{p'} = \overline{p}$ et $\overline{q'} = \overline{q}$ alors $p' \equiv p \pmod n$, $q' \equiv q \pmod n$ et donc $p' + q' \equiv p + q \pmod n$. Donc $\overline{p'+q'} = \overline{p+q}$. Donc on a aussi $\overline{p'} + \overline{q'} = \overline{p} + \overline{q}$. Nous avons montré que l'addition est indépendante du choix des représentants.

L'exemple de la vie courante est le suivant : considérons seulement les minutes d'une montre ; ces minutes varient de 0 à 59. Lorsque l'aiguille passe à 60, elle désigne aussi 0 (on ne s'occupe pas des heures). Ainsi de suite : 61 s'écrit aussi 1, 62 s'écrit aussi 2,... Cela correspond donc à l'ensemble $\mathbb{Z}/60\mathbb{Z}$. On peut aussi additionner des minutes : 50 minutes plus 15 minutes font 65 minutes qui s'écrivent aussi 5 minutes. Continuons avec l'écriture dans $\mathbb{Z}/60\mathbb{Z}$ par exemple : $\overline{135} + \overline{50} = \overline{185} = \overline{5}$. Remarquez que si l'on écrit d'abord $\overline{135} = \overline{15}$ alors $\overline{135} + \overline{50} = \overline{15} + \overline{50} = \overline{65} = \overline{5}$. On pourrait même écrire $\overline{50} = \overline{-10}$ et donc $\overline{135} + \overline{50} = \overline{15} - \overline{10} = \overline{5}$. C'est le fait que l'addition soit bien définie qui justifie que l'on trouve toujours le même résultat.

Proposition 95

$(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe commutatif.

C'est facile. L'élément neutre est $\overline{0}$. L'opposé de $\overline{k}$ est $-\overline{k}=\overline{-k}=\overline{n-k}$. L'associativité et la commutativité découlent de celles de $(\mathbb{Z},+)$.

4.2. Groupes cycliques de cardinal fini

Définition 74

Un groupe $(G,\star)$ est un groupe ***cyclique*** s'il existe un élément $a\in G$ tel que :

$$\text{pour tout } x\in G, \text{ il existe } k\in\mathbb{Z} \text{ tel que } x=a^k$$

Autrement dit le groupe G est engendré par un seul élément a.
Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe cyclique. En effet il est engendré par $a=\overline{1}$, car tout élément $\overline{k}$ s'écrit $\overline{k}=\underbrace{\overline{1}+\overline{1}+\cdots\overline{1}}_{k \text{ fois}}=k\cdot\overline{1}$.
Voici un résultat intéressant : il n'existe, à isomorphisme près, qu'un seul groupe cyclique à n éléments, c'est $\mathbb{Z}/n\mathbb{Z}$:

Théorème 41

Si $(G,\star)$ un groupe cyclique de cardinal n, alors $(G,\star)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

Démonstration

Comme G est cyclique alors $G=\{\ldots,a^{-2},a^{-1},e,a,a^2,a^3,\ldots\}$. Dans cette écriture il y a de nombreuses redondances (car de toute façon G n'a que n éléments). Nous allons montrer qu'en fait

$$G=\{e,a,a^2,\ldots,a^{n-1}\} \quad \text{et que} \quad a^n=e.$$

Tout d'abord l'ensemble $\{e,a,a^2,\ldots,a^{n-1}\}$ est inclus dans G. En plus il a exactement n éléments. En effet si $a^p=a^q$ avec $0\leqslant q<p\leqslant n-1$ alors $a^{p-q}=e$ (avec $p-q>0$) et ainsi $a^{p-q+1}=a^{p-q}\star a=a$, $a^{p-q+2}=a^2$ et alors le groupe G serait égal à $\{e,a,a^2,\ldots,a^{p-q-1}\}$ et n'aurait pas n éléments. Ainsi $\{e,a,a^2,\ldots,a^{n-1}\}\subset G$ et les deux ensembles ont le même nombre n d'éléments, donc ils sont égaux.
Montrons maintenant que $a^n=e$. Comme $a^n\in G$ et que $G=\{e,a,a^2,\ldots,a^{n-1}\}$ alors il existe $0\leqslant p\leqslant n-1$ tel que $a^n=a^p$. Encore une fois si $p>0$ cela entraîne $a^{n-p}=e$ et donc une contradiction. Ainsi $p=0$ donc $a^n=a^0=e$.

Nous pouvons maintenant construire l'isomorphisme entre $(\mathbb{Z}/n\mathbb{Z},+)$ et $(G,\star)$. Soit $f:\mathbb{Z}/n\mathbb{Z}\longrightarrow G$ l'application définie par $f(\overline{k})=a^k$.

- Il faut tout d'abord montrer que f est bien définie car notre définition de f dépend du représentant k et pas de la classe $\overline{k}$: si $\overline{k}=\overline{k'}$ (une même classe définie par deux représentants distincts) alors $k\equiv k' \pmod n$ et donc il existe $\ell\in\mathbb{Z}$ tel que $k=k'+\ell n$. Ainsi $f(\overline{k})=a^k=a^{k'+\ell n}=a^{k'}\star a^{\ell n}=a^{k'}\star(a^n)^\ell=a^{k'}\star e^\ell=a^{k'}=f(\overline{k'})$. Ainsi f est bien définie.
- f est un morphisme de groupes car $f(\overline{k}+\overline{k'})=f(\overline{k+k'})=a^{k+k'}=a^k\star a^{k'}=f(\overline{k})\star f(\overline{k'})$ (pour tout $x,x'\in\mathbb{Z}$).
- Il est clair que f est surjective car tout élément de G s'écrit a^k.
- Comme l'ensemble de départ et celui d'arrivée ont le même nombre d'éléments et que f est surjective alors f est bijective.

Conclusion f est un isomorphisme entre $(\mathbb{Z}/n\mathbb{Z},+)$ et $(G,\star)$.

Mini-exercices

1. Trouver tous les sous-groupes de $(\mathbb{Z}/12\mathbb{Z},+)$.
2. Montrer que le produit défini par $\overline{p}\times\overline{q}=\overline{p\times q}$ est bien défini sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$.
3. Dans la preuve du théorème 41, montrer directement que l'application f est injective.
4. Montrer que l'ensemble $\mathbb{U}_n=\left\{z\in\mathbb{C}\mid z^n=1\right\}$ est un sous-groupe de $(\mathbb{C}^*,\times)$. Montrer que $\mathbb{U}_n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Expliciter l'isomorphisme.
5. Montrer que l'ensemble $H=\left\{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right),\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)\right\}$ est un sous-groupe de $(\mathscr{GL}_2,\times)$ ayant 4 éléments. Montrer que H *n'est pas* isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

5. Le groupe des permutations $\mathscr{S}_n$

Fixons un entier $n\geqslant 2$.

5.1. Groupe des permutations

Proposition 96

L'ensemble des bijections de $\{1,2,\dots,n\}$ dans lui-même, muni de la composition des fonctions est un groupe, noté $(\mathscr{S}_n,\circ)$.

Une bijection de $\{1,2,\dots,n\}$ (dans lui-même) s'appelle une ***permutation***. Le groupe $(\mathscr{S}_n,\circ)$ s'appelle le ***groupe des permutations*** (ou le ***groupe symétrique***).

Démonstration

1. La composition de deux bijections de $\{1,2,\dots,n\}$ est une bijection de $\{1,2,\dots,n\}$.
2. La loi est associative (par l'associativité de la composition des fonctions).
3. L'élément neutre est l'identité.
4. L'inverse d'une bijection f est sa bijection réciproque f^{-1}.

Il s'agit d'un autre exemple de groupe ayant un nombre fini d'éléments :

Lemme 8

Le cardinal de $\mathscr{S}_n$ est $n!$.

Démonstration

La preuve est simple. Pour l'élément 1, son image appartient à $\{1,2,\dots,n\}$ donc nous avons n choix. Pour l'image de 2, il ne reste plus que $n-1$ choix (1 et 2 ne doivent pas avoir la même image car notre application est une bijection). Ainsi de suite... Pour l'image du dernier élément n il ne reste qu'une possibilité. Au final il y a $n \times (n-1) \times \cdots \times 2 \times 1 = n!$ façon de construire des bijections de $\{1,2,\dots,n\}$

5.2. Notation et exemples

Décrire une permutation $f : \{1,2,\dots,n\} \longrightarrow \{1,2,\dots,n\}$ équivaut à donner les images de chaque i allant de 1 à n. Nous notons donc f par

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{bmatrix}$$

Par exemple la permutation de $\mathcal{S}_7$ notée

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{bmatrix} f$$

est la bijection $f : \{1,2,\dots,7\} \longrightarrow \{1,2,\dots,7\}$ définie par $f(1)=3$, $f(2)=7$, $f(3)=5$, $f(4)=4$, $f(5)=6$, $f(6)=1$, $f(7)=2$. C'est bien une bijection car chaque nombre de 1 à 7 apparaît une fois et une seule sur la deuxième ligne.

L'élément neutre du groupe est l'identité id ; pour $\mathcal{S}_7$ c'est donc $\left[\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 1&2&3&4&5&6&7 \end{smallmatrix}\right]$.
Il est facile de calculer la composition de deux permutations f et g avec cette notation. Si $f = \left[\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 3&7&5&4&6&1&2 \end{smallmatrix}\right]$ et $g = \left[\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 4&3&2&1&7&5&6 \end{smallmatrix}\right]$ alors $g \circ f$ s'obtient en superposant la permutation f puis g

$$g \circ f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \not 3 & \not 7 & \not 5 & \not 4 & \not 6 & \not 1 & \not 2 \\ 2 & 6 & 7 & 1 & 5 & 4 & 3 \end{bmatrix} \begin{matrix} f \\ g \end{matrix} \; g \circ f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 7 & 1 & 5 & 4 & 3 \end{bmatrix}$$

ensuite on élimine la ligne intermédiaire du milieu et donc $g \circ f$ se note $\left[\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 2&6&7&1&5&4&3 \end{smallmatrix}\right]$.
Il est tout aussi facile de calculer l'inverse d'une permutation : il suffit d'échanger les lignes du haut et du bas et de réordonner le tableau. Par exemple l'inverse de

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{bmatrix} f^{-1}$$

se note $f^{-1} = \left[\begin{smallmatrix} 3&7&5&4&6&1&2 \\ 1&2&3&4&5&6&7 \end{smallmatrix}\right]$ ou plutôt après réordonnement $\left[\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 6&7&1&4&3&5&2 \end{smallmatrix}\right]$.

5.3. Le groupe $\mathcal{S}_3$

Nous allons étudier en détails le groupe $\mathcal{S}_3$ des permutations de $\{1,2,3\}$. Nous savons que $\mathcal{S}_3$ possède $3! = 6$ éléments que nous énumérons :

- $\mathrm{id} = \left[\begin{smallmatrix} 1&2&3 \\ 1&2&3 \end{smallmatrix}\right]$ l'identité,
- $\tau_1 = \left[\begin{smallmatrix} 1&2&3 \\ 1&3&2 \end{smallmatrix}\right]$ une transposition,
- $\tau_2 = \left[\begin{smallmatrix} 1&2&3 \\ 3&2&1 \end{smallmatrix}\right]$ une deuxième transposition,
- $\tau_3 = \left[\begin{smallmatrix} 1&2&3 \\ 2&1&3 \end{smallmatrix}\right]$ une troisième transposition,
- $\sigma = \left[\begin{smallmatrix} 1&2&3 \\ 2&3&1 \end{smallmatrix}\right]$ un cycle,
- $\sigma^{-1} = \left[\begin{smallmatrix} 1&2&3 \\ 3&1&2 \end{smallmatrix}\right]$ l'inverse du cycle précédent.

Donc $\mathscr{S}_3 = \{id, \tau_1, \tau_2, \tau_3, \sigma, \sigma^{-1}\}$.

Calculons $\tau_1 \circ \sigma$ et $\sigma \circ \tau_1$:

$$\tau_1 \circ \sigma = \begin{bmatrix} 1&2&3 \\ 2&3&1 \\ 3&2&1 \end{bmatrix} = \begin{bmatrix} 1&2&3 \\ 3&2&1 \end{bmatrix} = \tau_2 \quad \text{et} \quad \sigma \circ \tau_1 = \begin{bmatrix} 1&2&3 \\ 1&3&2 \\ 2&1&3 \end{bmatrix} = \begin{bmatrix} 1&2&3 \\ 2&1&3 \end{bmatrix} = \tau_3.$$

Ainsi $\tau_1 \circ \sigma = \tau_2$ est différent de $\sigma \circ \tau_1 = \tau_3$, ainsi le groupe $\mathscr{S}_3$ n'est pas commutatif. Et plus généralement :

Lemme 9

Pour $n \geqslant 3$, le groupe $\mathscr{S}_n$ n'est pas commutatif.

Nous pouvons calculer la table du groupe $\mathscr{S}_3$

$g \circ f$	id	τ_1	τ_2	τ_3	σ	σ^{-1}
id	id	τ_1	τ_2	τ_3	σ	σ^{-1}
τ_1	τ_1	id	σ	σ^{-1}	$\tau_1 \circ \sigma = \tau_2$	τ_3
τ_2	τ_2	σ^{-1}	id	σ	τ_3	τ_1
τ_3	τ_3	σ	σ^{-1}	id	τ_1	τ_2
σ	σ	$\sigma \circ \tau_1 = \tau_3$	τ_1	τ_2	σ^{-1}	id
σ^{-1}	σ^{-1}	τ_2	τ_3	τ_1	id	σ

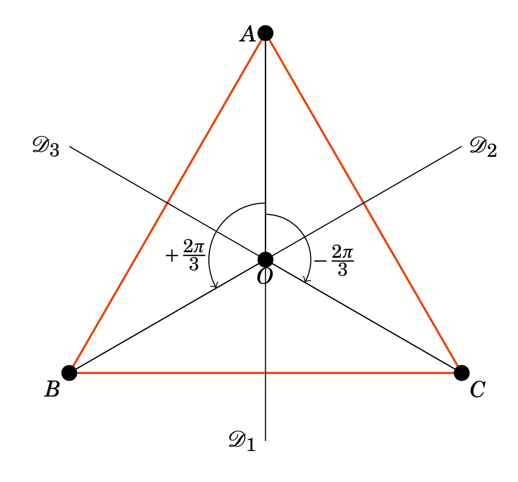
FIGURE 14.1 – Table du groupe $\mathscr{S}_3$

Comment avons-nous rempli cette table ? Nous avons déjà calculé $\tau_1 \circ \sigma = \tau_2$ et $\sigma \circ \tau_1 = \tau_3$. Comme $f \circ id = f$ et $\text{id} \circ f = f$ il est facile de remplir la première colonne noire ainsi que la première ligne noire. Ensuite il faut faire les calculs !

On retrouve ainsi que $\mathscr{S}_3 = \{id, \tau_1, \tau_2, \tau_3, \sigma, \sigma^{-1}\}$ est un groupe : en particulier la composition de deux permutations de la liste reste une permutation de la liste. On lit aussi sur la table l'inverse de chaque élément, par exemple sur la ligne de τ_2 on cherche à quelle colonne on trouve l'identité, c'est la colonne de τ_2. Donc l'inverse de τ_2 est lui-même.

5.4. Groupe des isométries du triangle

Soit (ABC) un triangle équilatéral. Considérons l'ensemble des isométries du plan qui préservent le triangle, c'est-à-dire que l'on cherche toutes les isométries f telles que $f(A) \in \{A, B, C\}$, $f(B) \in \{A, B, C\}$, $f(C) \in \{A, B, C\}$. On trouve les isométries suivantes : l'identité id, les réflexions t_1, t_2, t_3 d'axes $\mathscr{D}_1, \mathscr{D}_2, \mathscr{D}_3$, la rotation s d'angle $\frac{2\pi}{3}$ et la rotation s^{-1} d'angle $-\frac{2\pi}{3}$ (de centre O).



Proposition 97

L'ensemble des isométries d'un triangle équilatéral, muni de la composition, forme un groupe. Ce groupe est isomorphe à $(\mathscr{S}_3, \circ)$.

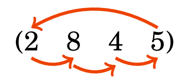
L'isomorphisme est juste l'application qui à t_i associe τ_i, à s associe σ et à s^{-1} associe σ^{-1}.

5.5. Décomposition en cycles

- Nous allons définir ce qu'est un ***cycle*** : c'est une permutation σ qui fixe un certain nombre d'éléments ($\sigma(i) = i$) et dont les éléments non fixés sont obtenus par itération : $j, \sigma(j), \sigma^2(j), \ldots$ C'est plus facile à comprendre sur un exemple :

$$\sigma = \begin{bmatrix} 1 & \mathbf{2} & 3 & \mathbf{4} & \mathbf{5} & 6 & 7 & \mathbf{8} \\ 1 & \mathbf{8} & 3 & \mathbf{5} & \mathbf{2} & 6 & 7 & \mathbf{4} \end{bmatrix}$$

  est un cycle : les éléments $1,3,6,7$ sont fixes, les autres s'obtiennent comme itération de 2 : $2 \mapsto \sigma(2) = 8 \mapsto \sigma(8) = \sigma^2(2) = 4 \mapsto \sigma(4) = \sigma^3(2) = 5$, ensuite on retrouve $\sigma^4(2) = \sigma(5) = 2$.
- Nous noterons ce cycle par



  Il faut comprendre cette notation ainsi : l'image de 2 est 8, l'image de 8 est 4, l'image de 4 est 5, l'image de 5 est 2. Les éléments qui n'apparaissent pas (ici $1,3,6,7$) sont fixes. On aurait pu aussi noter ce même cycle par : $(8\ 4\ 5\ 2)$, $(4\ 5\ 2\ 8)$ ou $(5\ 2\ 8\ 4)$.
- Pour calculer l'inverse on renverse les nombres : l'inverse de $\sigma = (2\ 8\ 4\ 5)$ est $\sigma^{-1} = (5\ 4\ 8\ 2)$.
- Le ***support*** d'un cycle sont les éléments qui ne sont pas fixes : le support de σ est $\{2,4,5,8\}$. La ***longueur*** (ou l'***ordre***) d'un cycle est le nombre d'éléments qui ne sont pas fixes (c'est donc le cardinal du support). Par exemple $(2\ 8\ 4\ 5)$ est un cycle de longueur 4.
- Autres exemples : $\sigma = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right] = (1\ 2\ 3)$ est un cycle de longueur 3 ; $\tau = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{smallmatrix}\right] = (2\ 4)$ est un cycle de longueur 2, aussi appelé une ***transposition***.
- Par contre $f = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 5 & 4 & 6 & 3 & 1 \end{smallmatrix}\right]$ n'est pas un cycle ; il s'écrit comme la composition de deux cycles $f = (1\ 7) \circ (3\ 5\ 6)$. Comme les supports de $(1\ 7)$ et $(3\ 5\ 6)$ sont disjoints alors on a aussi $f = (3\ 5\ 6) \circ (1\ 7)$.

Ce dernier point fait partie d'un résultat plus général que nous admettons :

Théorème 42

Toute permutation de $\mathscr{S}_n$ se décompose en composition de cycles à supports disjoints. De plus cette décomposition est unique.

Pour l'unicité il faut comprendre : unique à l'écriture de chaque cycle près (exemple : $(3\ 5\ 6)$ et $(5\ 6\ 3)$ sont le même cycle) et à l'ordre près (exemple : $(1\ 7) \circ (3\ 5\ 6) = (3\ 5\ 6) \circ (1\ 7)$).
Exemple : la décomposition de $f = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 8 & 3 & 7 & 6 & 4 \end{smallmatrix}\right]$ en composition de cycle à supports disjoints est $(1\ 5\ 3) \circ (4\ 8) \circ (6\ 7)$.

Attention, si les supports ne sont pas disjoints alors cela ne commute plus : par exemple $g = (1\ 2) \circ (2\ 3\ 4)$ n'est pas égale à $h = (2\ 3\ 4) \circ (1\ 2)$. En effet l'écriture de g en produit de cycle à support disjoint est $g = (1\ 2) \circ (2\ 3\ 4) = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right] = (1\ 2\ 3\ 4)$ alors que celle de h est $h = (2\ 3\ 4) \circ (1\ 2) = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{smallmatrix}\right] = (1\ 3\ 4\ 2)$.

Mini-exercices

1. Soient f définie par $f(1) = 2$, $f(2) = 3$, $f(3) = 4$, $f(4) = 5$, $f(5) = 1$ et g définie par $g(1) = 2$, $g(2) = 1$, $g(3) = 4$, $g(4) = 3$, $g(5) = 5$. Écrire les permutations f, g, f^{-1}, g^{-1}, $g \circ f$, $f \circ g$, f^2, g^2, $(g \circ f)^2$.
2. Énumérer toutes les permutations de $\mathscr{S}_4$ qui n'ont pas d'éléments fixes. Les écrire ensuite sous forme de compositions de cycles à supports disjoints.
3. Trouver les isométries directes préservant un carré. Dresser la table des compositions et montrer qu'elles forment un groupe. Montrer que ce groupe est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.
4. Montrer qu'il existe un sous-groupe de $\mathscr{S}_3$ isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Même question avec $\mathbb{Z}/3\mathbb{Z}$. Est-ce que $\mathscr{S}_3$ et $\mathbb{Z}/6\mathbb{Z}$ sont isomorphes ?
5. Décomposer la permutation suivante en produit de cycles à supports disjoints : $f = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 2 & 6 & 1 & 4 & 3 \end{smallmatrix}\right]$. Calculer f^2, f^3, f^4 puis f^{20xx} où $20xx$ est l'année en cours. Mêmes questions avec $g = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 9 & 6 & 5 & 2 & 4 & 7 & 1 \end{smallmatrix}\right]$ et $h = (25)(1243)(12)$.

Auteurs

Arnaud Bodin
Benjamin Boutin
Pascal Romon

Exo7

15 Systèmes linéaires

Vidéo ■ partie 1. Introduction aux systèmes d'équations linéaires
Vidéo ■ partie 2. Théorie des systèmes linéaires
Vidéo ■ partie 3. Résolution par la méthode du pivot de Gauss

1. Introduction aux systèmes d'équations linéaires

L'algèbre linéaire est un outil essentiel pour toutes les branches des mathématiques appliquées, en particulier lorsqu'il s'agit de modéliser puis résoudre numériquement des problèmes issus de divers domaines : des sciences physiques ou mécaniques, des sciences du vivant, de la chimie, de l'économie, des sciences de l'ingénieur,...
Les systèmes linéaires interviennent dans de nombreux contextes d'applications car ils forment la base calculatoire de l'algèbre linéaire. Ils permettent également de traiter une bonne partie de la théorie de l'algèbre linéaire en dimension finie. C'est pourquoi le présent cours commence avec une étude des équations linéaires et de leur résolution.
Ce chapitre a un but essentiellement pratique : résoudre des systèmes linéaires. La partie théorique sera revue et prouvée dans le chapitre « Matrices ».

1.1. Exemple : deux droites dans le plan

L'équation d'une droite dans le plan (Oxy) s'écrit

$$ax + by = e$$

où a, b et e sont des paramètres réels. Cette équation s'appelle ***équation linéaire*** dans les variables (ou inconnues) x et y.

Par exemple, $2x + 3y = 6$ est une équation linéaire, alors que les équations suivantes ne sont pas des équations linéaires :

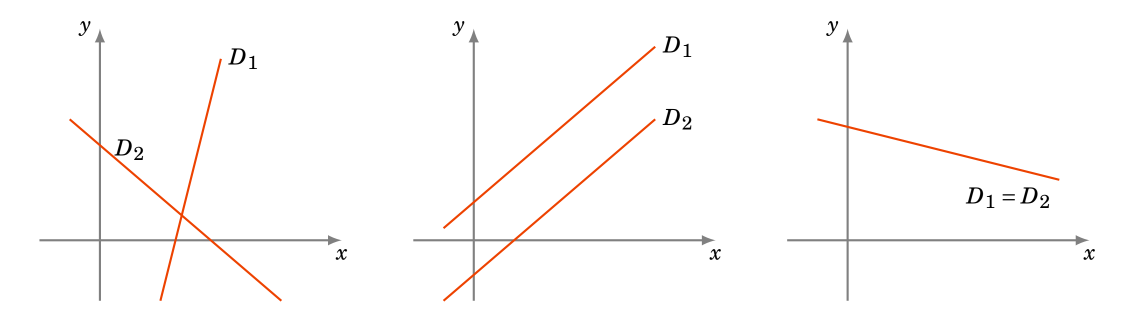
$$2x + y^2 = 1 \quad \text{ou} \quad y = \sin(x) \quad \text{ou} \quad x = \sqrt{y}.$$

Considérons maintenant deux droites D_1 et D_2 et cherchons les points qui sont simultanément sur ces deux droites. Un point (x, y) est dans l'intersection $D_1 \cap D_2$ s'il est solution du système :

$$\begin{cases} ax + by = e \\ cx + dy = f \end{cases} \qquad (S)$$

Trois cas se présentent alors :

1. Les droites D_1 et D_2 se coupent en un seul point. Dans ce cas, illustré par la figure de gauche, le système (S) a une seule solution.
2. Les droites D_1 et D_2 sont parallèles. Alors le système (S) n'a pas de solution. La figure du centre illustre cette situation.
3. Les droites D_1 et D_2 sont confondues et, dans ce cas, le système (S) a une infinité de solutions.



Nous verrons plus loin que ces trois cas de figure (une seule solution, aucune solution, une infinité de solutions) sont les seuls cas qui peuvent se présenter pour n'importe quel système d'équations linéaires.

1.2. Résolution par substitution

Pour savoir s'il existe une ou plusieurs solutions à un système linéaire, et les calculer, une première méthode est la ***substitution***. Par exemple pour le système :

$$\begin{cases} 3x+2y &= 1 \\ 2x-7y &= -2 \end{cases} \qquad (S)$$

Nous réécrivons la première ligne $3x+2y=1$ sous la forme $y=\frac{1}{2}-\frac{3}{2}x$. Et nous remplaçons (nous *substituons*) le y de la seconde équation, par l'expression $\frac{1}{2}-\frac{3}{2}x$. Nous obtenons un système équivalent :

$$\begin{cases} y &= \frac{1}{2}-\frac{3}{2}x \\ 2x-7(\frac{1}{2}-\frac{3}{2}x) &= -2 \end{cases}$$

La seconde équation est maintenant une expression qui ne contient que des x, et on peut la résoudre :

$$\begin{cases} y &= \frac{1}{2}-\frac{3}{2}x \\ (2+7\times\frac{3}{2})x &= -2+\frac{7}{2} \end{cases} \iff \begin{cases} y &= \frac{1}{2}-\frac{3}{2}x \\ x &= \frac{3}{25} \end{cases}$$

Il ne reste plus qu'à remplacer dans la première ligne la valeur de x obtenue :

$$\begin{cases} y &= \frac{8}{25} \\ x &= \frac{3}{25} \end{cases}$$

Le système (S) admet donc une solution unique $(\frac{3}{25},\frac{8}{25})$. L'ensemble des solutions est donc

$$\mathscr{S}=\left\{\left(\frac{3}{25},\frac{8}{25}\right)\right\}.$$

1.3. Exemple : deux plans dans l'espace

Dans l'espace $(0xyz)$, une équation linéaire est l'équation d'un plan :

$$ax+by+cz=d$$

L'intersection de deux plans dans l'espace correspond au système suivant à 2 équations et à 3 inconnues :

$$\begin{cases} ax+by+cz &= d \\ a'x+b'y+c'z &= d' \end{cases}$$

Trois cas se présentent alors :

- les plans sont parallèles (et distincts) et il n'y a alors aucune solution au système,
- les plans sont confondus et il y a une infinité de solutions au système,
- les plans se coupent en une droite et il y a une infinité de solutions.

Exemple 145

1. Le système $\begin{cases} 2x+3y-4z &= 7 \\ 4x+6y-8z &= -1 \end{cases}$ n'a pas de solution. En effet, en divisant par 2 la seconde équation, on obtient le système équivalent : $\begin{cases} 2x+3y-4z &= 7 \\ 2x+3y-4z &= -\frac{1}{2} \end{cases}$. Les deux lignes sont clairement incompatibles : aucun (x,y,z) ne peut vérifier à la fois $2x+3y-4z=7$ et $2x+3y-4z=-\frac{1}{2}$. L'ensemble des solutions est donc $\mathscr{S}=\varnothing$.
2. Pour le système $\begin{cases} 2x+3y-4z &= 7 \\ 4x+6y-8z &= 14 \end{cases}$, les deux équations définissent le même plan ! Le système est donc équivalent à une seule équation : $2x+3y-4z=7$. Si on récrit cette équation sous la forme $z=\frac{1}{2}x+\frac{3}{4}y-\frac{7}{4}$, alors on peut décrire l'ensemble des solutions sous la forme : $\mathscr{S}=\{(x,y,\frac{1}{2}x+\frac{3}{4}y-\frac{7}{4})\mid x,y\in\mathbb{R}\}$.
3. Soit le système $\begin{cases} 7x+2y-2z &= 1 \\ 2x+3y+2z &= 1 \end{cases}$. Par substitution :

$$\begin{cases} 7x+2y-2z=1 \\ 2x+3y+2z=1 \end{cases} \iff \begin{cases} z=\frac{7}{2}x+y-\frac{1}{2} \\ 2x+3y+2(\frac{7}{2}x+y-\frac{1}{2})=1 \end{cases} \iff \begin{cases} z=\frac{7}{2}x+y-\frac{1}{2} \\ 9x+5y=2 \end{cases}$$

$$\iff \begin{cases} z=\frac{7}{2}x+y-\frac{1}{2} \\ y=-\frac{9}{5}x+\frac{2}{5} \end{cases} \iff \begin{cases} z=\frac{17}{10}x-\frac{1}{10} \\ y=-\frac{9}{5}x+\frac{2}{5} \end{cases}$$

Pour décrire l'ensemble des solutions, on peut choisir x comme paramètre :

$$\mathscr{S}=\left\{\left(x,-\frac{9}{5}x+\frac{2}{5},\frac{17}{10}x-\frac{1}{10}\right)\mid x\in\mathbb{R}\right\}.$$

Géométriquement : nous avons trouvé une équation paramétrique de la droite définie par l'intersection de deux plans.

Du point de vue du nombre de solutions, nous constatons qu'il n'y a que deux possibilités, à savoir aucune solution ou une infinité de solutions. Mais les deux derniers cas ci-dessus sont néanmoins très différents géométriquement et il semblerait que dans le second cas (plans confondus), l'infinité de solutions soit plus grande que dans le troisième cas. Les chapitres suivants nous permettront de rendre rigoureuse cette impression.

Si on considère trois plans dans l'espace, une autre possibilité apparaît : il se peut que les trois plans s'intersectent en un seul point.

1.4. Résolution par la méthode de Cramer

On note $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$ le ***déterminant***. On considère le cas d'un système de 2 équations à 2 inconnues :

$$\begin{cases} ax + by &= e \\ cx + dy &= f \end{cases}$$

Si $ad - bc \neq 0$, on trouve une unique solution dont les coordonnées (x, y) sont :

$$x = \frac{\begin{vmatrix} e & b \\ f & d \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}} \qquad y = \frac{\begin{vmatrix} a & e \\ c & f \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}$$

Notez que le dénominateur égale le déterminant pour les deux coordonnées et est donc non nul. Pour le numérateur de la première coordonnée x, on remplace la première colonne par le second membre ; pour la seconde coordonnée y, on remplace la seconde colonne par le second membre.

Exemple 146

Résolvons le système $\begin{cases} tx - 2y &= 1 \\ 3x + ty &= 1 \end{cases}$ suivant la valeur du paramètre $t \in \mathbb{R}$.
Le déterminant associé au système est $\begin{vmatrix} t & -2 \\ 3 & t \end{vmatrix} = t^2 + 6$ et ne s'annule jamais. Il existe donc une unique solution (x, y) et elle vérifie :

$$x = \frac{\begin{vmatrix} 1 & -2 \\ 1 & t \end{vmatrix}}{t^2 + 6} = \frac{t + 2}{t^2 + 6}, \qquad y = \frac{\begin{vmatrix} t & 1 \\ 3 & 1 \end{vmatrix}}{t^2 + 6} = \frac{t - 3}{t^2 + 6}.$$

Pour chaque t, l'ensemble des solutions est $\mathcal{S} = \left\{ \left(\frac{t+2}{t^2+6}, \frac{t-3}{t^2+6} \right) \right\}$.

1.5. Résolution par inversion de matrice

Pour ceux qui connaissent les matrices, le système linéaire

$$\begin{cases} ax + by &= e \\ cx + dy &= f \end{cases}$$

est équivalent à

$$AX = Y \quad \text{où} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad X = \begin{pmatrix} x \\ y \end{pmatrix}, \quad Y = \begin{pmatrix} e \\ f \end{pmatrix}.$$

Si le déterminant de la matrice A est non nul, c'est-à-dire si $ad - bc \neq 0$, alors la matrice A est inversible et

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

et l'unique solution $X = \binom{x}{y}$ du système est donnée par

$$X = A^{-1} Y.$$

Exemple 147

Résolvons le système $\begin{cases} x+y &= 1 \\ x+t^2y &= t \end{cases}$ suivant la valeur du paramètre $t \in \mathbb{R}$.

Le déterminant du système est $\begin{vmatrix} 1 & 1 \\ 1 & t^2 \end{vmatrix} = t^2-1$.

Premier cas. $t \neq +1$ **et** $t \neq -1$. Alors $t^2-1 \neq 0$. La matrice $A = \begin{pmatrix} 1 & 1 \\ 1 & t^2 \end{pmatrix}$ est inversible d'inverse $A^{-1} = \frac{1}{t^2-1}\begin{pmatrix} t^2 & -1 \\ -1 & 1 \end{pmatrix}$. Et la solution $X = \begin{pmatrix} x \\ y \end{pmatrix}$ est

$$X = A^{-1}Y = \frac{1}{t^2-1}\begin{pmatrix} t^2 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ t \end{pmatrix} = \frac{1}{t^2-1}\begin{pmatrix} t^2-t \\ t-1 \end{pmatrix} = \begin{pmatrix} \frac{t}{t+1} \\ \frac{1}{t+1} \end{pmatrix}.$$

Pour chaque $t \neq \pm 1$, l'ensemble des solutions est $\mathscr{S} = \left\{\left(\frac{t}{t+1}, \frac{1}{t+1}\right)\right\}$.

Deuxième cas. $t = +1$. Le système s'écrit alors : $\begin{cases} x+y &= 1 \\ x+y &= 1 \end{cases}$ et les deux équations sont identiques. Il y a une infinité de solutions : $\mathscr{S} = \{(x, 1-x) \mid x \in \mathbb{R}\}$.

Troisième cas. $t = -1$. Le système s'écrit alors : $\begin{cases} x+y &= 1 \\ x+y &= -1 \end{cases}$, les deux équations sont clairement incompatibles et donc $\mathscr{S} = \varnothing$.

Mini-exercices

1. Tracer les droites et résoudre le système linéaire $\begin{cases} x-2y &= -1 \\ -x+3y &= 3 \end{cases}$ de trois façons différentes : substitution, méthode de Cramer, inverse d'une matrice. Idem avec $\begin{cases} 2x-y &= 4 \\ 3x+3y &= -5 \end{cases}$.
2. Résoudre suivant la valeur du paramètre $t \in \mathbb{R}$: $\begin{cases} 4x-3y &= t \\ 2x-y &= t^2 \end{cases}$.
3. Discuter et résoudre suivant la valeur du paramètre $t \in \mathbb{R}$: $\begin{cases} tx-y &= 1 \\ x+(t-2)y &= -1 \end{cases}$. Idem avec $\begin{cases} (t-1)x+y &= 1 \\ 2x+ty &= -1 \end{cases}$.

2. Théorie des systèmes linéaires

2.1. Définitions

Définition 75

On appelle ***équation linéaire*** dans les variables (ou ***inconnues***) $x_1, \ldots, x_p$ toute relation de la forme

$$a_1x_1 + \cdots + a_px_p = b, \tag{15.1}$$

où $a_1, \ldots, a_p$ et b sont des nombres réels donnés.

Remarque

- Il importe d'insister ici sur le fait que ces équations linéaires sont *implicites*, c'est-à-dire qu'elles décrivent des relations entre les variables, mais ne donnent pas directement les valeurs que peuvent prendre les variables.
- *Résoudre* une équation signifie donc la rendre *explicite*, c'est-à-dire rendre plus apparentes les valeurs que les variables peuvent prendre.
- On peut aussi considérer des équations linéaires de nombres rationnels ou de nombres complexes.

Soit $n \geqslant 1$ un entier.

Définition 76

Un ***système de n équations linéaires à p inconnues*** est une liste de n équations linéaires.

On écrit usuellement de tels systèmes en n lignes placées les unes sous les autres.

Exemple 148

Le système suivant a 2 équations et 3 inconnues :

$$\begin{cases} x_1 & - & 3x_2 & + & x_3 & = & 1 \\ -2x_1 & + & 4x_2 & - & 3x_3 & = & 9 \end{cases}$$

La forme générale d'un système linéaire de n équations à p inconnues est la suivante :

$$\begin{cases} a_{11}x_1 & +a_{12}x_2 & +a_{13}x_3 & + & \cdots & +a_{1p}x_p & = & b_1 & (\leftarrow \text{équation } 1) \\ a_{21}x_1 & +a_{22}x_2 & +a_{23}x_3 & + & \cdots & +a_{2p}x_p & = & b_2 & (\leftarrow \text{équation } 2) \\ \vdots & \vdots & \vdots & & & \vdots & = & \vdots & \\ a_{i1}x_1 & +a_{i2}x_2 & +a_{i3}x_3 & + & \cdots & +a_{ip}x_p & = & b_i & (\leftarrow \text{équation } i) \\ \vdots & \vdots & \vdots & & & \vdots & = & \vdots & \\ a_{n1}x_1 & +a_{n2}x_2 & +a_{n3}x_3 & + & \cdots & +a_{np}x_p & = & b_n & (\leftarrow \text{équation } n) \end{cases}$$

Les nombres a_{ij}, $i = 1,\dots,n$, $j = 1,\dots,p$, sont les ***coefficients*** du système. Ce sont des données. Les nombres b_i, $i = 1,\dots,n$, constituent le ***second membre*** du système et sont également des données. Il convient de bien observer comment on a rangé le système en lignes (une ligne par équation) numérotées de 1 à n par l'indice i, et en colonnes : les termes correspondant à une même inconnue x_j sont alignés verticalement les uns sous les autres. L'indice j varie de 1 à p. Il y a donc p colonnes à gauche des signes d'égalité, plus une colonne supplémentaire à droite pour le second membre. La notation avec double indice a_{ij} correspond à ce rangement : le *premier* indice (ici i) est le numéro de *ligne* et le *second* indice (ici j) est le numéro de *colonne*. Il est extrêmement important de toujours respecter cette convention.
Dans l'exemple 148, on a $n = 2$ (nombre d'équations = nombre de lignes), $p = 3$ (nombre d'inconnues = nombre de colonnes à gauche du signe =) et $a_{11} = 1$, $a_{12} = -3$, $a_{13} = 1$, $a_{21} = -2$, $a_{22} = 4$, $a_{23} = -3$, $b_1 = 1$ et $b_2 = 9$.

Définition 77

Une ***solution*** du système linéaire est une liste de p nombres réels $(s_1, s_2, \dots, s_p)$ (un p-uplet) tels que si l'on substitue s_1 pour x_1, s_2 pour x_2, etc., dans le système linéaire, on obtient une égalité. L'***ensemble des solutions du système*** est l'ensemble de tous ces p-uplets.

Exemple 149

Le système

$$\begin{cases} x_1 - 3x_2 + x_3 = 1 \\ -2x_1 + 4x_2 - 3x_3 = 9 \end{cases}$$

admet comme solution $(-18, -6, 1)$, c'est-à-dire

$$x_1 = -18, \qquad x_2 = -6, \qquad x_3 = 1.$$

Par contre, $(7, 2, 0)$ ne satisfait que la première équation. Ce n'est donc pas une solution du système.

En règle générale, on s'attache à déterminer l'ensemble des solutions d'un système linéaire. C'est ce que l'on appelle ***résoudre*** le système linéaire. Ceci amène à poser la définition suivante.

Définition 78

On dit que deux systèmes linéaires sont ***équivalents*** s'ils ont le même ensemble de solutions.

À partir de là, le jeu pour résoudre un système linéaire donné consistera à le transformer en un système équivalent dont la résolution sera plus simple que celle du système de départ. Nous verrons plus loin comment procéder de façon systématique pour arriver à ce but.

2.2. Différents types de systèmes

Voici un résultat théorique important pour les systèmes linéaires.

Théorème 43

Un système d'équations linéaires n'a soit aucune solution, soit une seule solution, soit une infinité de solutions.

En particulier, si vous trouvez 2 solutions différentes à un système linéaire, alors c'est que vous pouvez en trouver une infinité ! Un système linéaire qui n'a aucune solution est dit ***incompatible***. La preuve de ce théorème sera vue dans un chapitre ultérieur (« Matrices »).

2.3. Systèmes homogènes

Un cas particulier important est celui des ***systèmes homogènes***, pour lesquels $b_1 = b_2 = \cdots = b_n = 0$, c'est-à-dire dont le second membre est nul. De tels systèmes sont toujours compatibles car ils admettent toujours la solution $s_1 = s_2 = \cdots = s_p = 0$. Cette solution est appelée *solution triviale*. Géométriquement, dans le cas 2×2, un système homogène correspond à deux droites qui passent par l'origine, $(0, 0)$ étant donc toujours solution.

Mini-exercices

1. Écrire un système linéaire de 4 équations et 3 inconnues qui n'a aucune solution. Idem avec une infinité de solution. Idem avec une solution unique.
2. Résoudre le système à n équations et n inconnues dont les équations sont (L_i) : $x_i - x_{i+1} = 1$ pour $i = 1, \dots, n-1$ et (L_n) : $x_n = 1$.
3. Résoudre les systèmes suivants :

$$\begin{cases} x_1 & +2x_2 & +3x_3 & +4x_4 & = & 0 \\ & x_2 & +2x_3 & +3x_4 & = & 9 \\ & & x_3 & +2x_4 & = & 0 \end{cases} \quad \begin{cases} x_1 & +2x_2 & +3x_3 & = & 1 \\ x_1 & +x_2 & +x_3 & = & 2 \\ x_1 & -x_2 & +x_3 & = & 3 \end{cases} \quad \begin{cases} x_1 & +x_2 & & & = & 1 \\ & x_2 & +x_3 & & = & 2 \\ & & x_3 & +x_4 & = & 3 \\ x_1 & +2x_2 & +2x_3 & +x_4 & = & 0 \end{cases}$$

4. Montrer que si un système linéaire *homogène* a une solution $(x_1, \dots, x_p) \neq (0, \dots, 0)$, alors il admet une infinité de solutions.

3. Résolution par la méthode du pivot de Gauss

3.1. Systèmes échelonnés

Définition 79

Un système est ***échelonné*** si :

- le nombre de coefficients nuls commençant une ligne croît strictement ligne après ligne.

Il est ***échelonné réduit*** si en plus :

- le premier coefficient non nul d'une ligne vaut 1 ;
- et c'est le seul élément non nul de sa colonne.

Exemple 150

- $\begin{cases} 2x_1 & +3x_2 & +2x_3 & -x_4 & = & 5 \\ & -x_2 & -2x_3 & & = & 4 \\ & & & 3x_4 & = & 1 \end{cases}$ est échelonné (mais pas réduit).
- $\begin{cases} 2x_1 & +3x_2 & +2x_3 & -x_4 & = & 5 \\ & & -2x_3 & & = & 4 \\ & & x_3 & +x_4 & = & 1 \end{cases}$ n'est pas échelonné (la dernière ligne commence avec la même variable que la ligne au-dessus).

Il se trouve que les systèmes linéaires sous une forme échelonnée réduite sont particulièrement simples à résoudre.

Exemple 151

Le système linéaire suivant à 3 équations et 4 inconnues est échelonné et réduit.

$$\begin{cases} x_1 & & +2x_3 & & = & 25 \\ & x_2 & -2x_3 & & = & 16 \\ & & & x_4 & = & 1 \end{cases}$$

Ce système se résout trivialement en

$$\begin{cases} x_1 &= 25-2x_3 \\ x_2 &= 16+2x_3 \\ x_4 &= 1. \end{cases}$$

En d'autres termes, pour toute valeur de x_3 réelle, les valeurs de x_1, x_2 et x_4 calculées ci-dessus fournissent une solution du système, et on les a ainsi toutes obtenues. On peut donc décrire entièrement l'ensemble des solutions :

$$\mathscr{S} = \{(25-2x_3, 16+2x_3, x_3, 1) \mid x_3 \in \mathbb{R}\}.$$

3.2. Opérations sur les équations d'un système

Nous allons utiliser trois opérations élémentaires sur les équations (c'est-à-dire sur les lignes) qui sont :

1. $L_i \leftarrow \lambda L_i$ avec $\lambda \neq 0$: on peut multiplier une équation par un réel non nul.
2. $L_i \leftarrow L_i + \lambda L_j$ avec $\lambda \in \mathbb{R}$ (et $j \neq i$) : on peut ajouter à l'équation L_i un multiple d'une autre équation L_j.
3. $L_i \leftrightarrow L_j$: on peut échanger deux équations.

Ces trois opérations élémentaires ne changent pas les solutions d'un système linéaire ; autrement dit ces opérations transforment un système linéaire en un système linéaire équivalent.

Exemple 152

Utilisons ces opérations élémentaires pour résoudre le système suivant.

$$\begin{cases} x & +y & +7z & = & -1 & \quad (L_1) \\ 2x & -y & +5z & = & -5 & \quad (L_2) \\ -x & -3y & -9z & = & -5 & \quad (L_3) \end{cases}$$

Commençons par l'opération $L_2 \leftarrow L_2 - 2L_1$: on soustrait à la deuxième équation deux fois la première équation. On obtient un système équivalent avec une nouvelle deuxième ligne (plus simple) :

$$\begin{cases} x & +y & +7z & = & -1 & \\ & -3y & -9z & = & -3 & \quad L_2 \leftarrow L_2-2L_1 \\ -x & -3y & -9z & = & -5 & \end{cases}$$

Puis $L_3 \leftarrow L_3 + L_1$:

$$\begin{cases} x & +y & +7z & = & -1 & \\ & -3y & -9z & = & -3 & \\ & -2y & -2z & = & -6 & \quad L_3 \leftarrow L_3+L_1 \end{cases}$$

On continue pour faire apparaître un coefficient 1 en tête de la deuxième ligne ; pour cela on divise la ligne L_2 par -3 :

$$\begin{cases} x & +y & +7z & = & -1 & \\ & y & +3z & = & 1 & \quad L_2 \leftarrow -\frac{1}{3}L_2 \\ & -2y & -2z & = & -6 & \end{cases}$$

On continue ainsi

$$\begin{cases} x & +y & +7z & = & -1 \\ & y & +3z & = & 1 \\ & & 4z & = & -4 \end{cases} \qquad L_3 \leftarrow L_3 + 2L_2$$

$$\begin{cases} x & +y & +7z & = & -1 \\ & y & +3z & = & 1 \\ & & z & = & -1 \end{cases} \qquad L_3 \leftarrow \frac{1}{4}L_3$$

$$\begin{cases} x & +y & +7z & = & -1 \\ & y & & = & 4 \\ & & z & = & -1 \end{cases} \qquad L_2 \leftarrow L_2 - 3L_3$$

$$\begin{cases} x & +y & & = & 6 \\ & y & & = & 4 \\ & & z & = & -1 \end{cases} \qquad L_1 \leftarrow L_1 - 7L_3$$

On aboutit à un système réduit et échelonné :

$$\begin{cases} x & & & = & 2 \\ & y & & = & 4 \\ & & z & = & -1 \end{cases} \qquad L_1 \leftarrow L_1 - L_2$$

On obtient ainsi $x = 2$, $y = 4$ et $z = -1$ et l'unique solution du système est $(2, 4, -1)$.

La méthode utilisée pour cet exemple est reprise et généralisée dans le paragraphe suivant.

3.3. Méthode du pivot de Gauss

La méthode du pivot de Gauss permet de trouver les solutions de n'importe quel système linéaire. Nous allons décrire cet algorithme sur un exemple. Il s'agit d'une description précise d'une suite d'opérations à effectuer, qui dépendent de la situation et d'un ordre précis. Ce processus aboutit toujours (et en plus assez rapidement) à un système échelonné puis réduit, qui conduit immédiatement aux solutions du système.

Partie A. Passage à une forme échelonnée.

Soit le système suivant à résoudre :

$$\begin{cases} & -x_2 & +2x_3 & +13x_4 & = & 5 \\ x_1 & -2x_2 & +3x_3 & +17x_4 & = & 4 \\ -x_1 & +3x_2 & -3x_3 & -20x_4 & = & -1 \end{cases}$$

Pour appliquer la méthode du pivot de Gauss, il faut d'abord que le premier coefficient de la première ligne soit non nul. Comme ce n'est pas le cas ici, on échange les deux premières lignes par l'opération élémentaire $L_1 \leftrightarrow L_2$:

$$\begin{cases} x_1 & -2x_2 & +3x_3 & +17x_4 & = & 4 \\ & -x_2 & +2x_3 & +13x_4 & = & 5 \\ -x_1 & +3x_2 & -3x_3 & -20x_4 & = & -1 \end{cases} \qquad L_1 \leftrightarrow L_2$$

Nous avons déjà un coefficient 1 devant le x_1 de la première ligne. On dit que nous avons un ***pivot*** en position $(1, 1)$ (première ligne, première colonne). Ce pivot sert de base pour éliminer tous les autres termes sur la même colonne.

Il n'y a pas de terme x_1 sur le deuxième ligne. Faisons disparaître le terme x_1 de la troisième ligne ; pour cela on fait l'opération élémentaire $L_3 \leftarrow L_3 + L_1$:

$$\begin{cases} x_1 & -2x_2 & +3x_3 & +17x_4 & = & 4 \\ & -x_2 & +2x_3 & +13x_4 & = & 5 \\ & x_2 & & -3x_4 & = & 3 \end{cases} \qquad L_3 \leftarrow L_3 + L_1$$

On change le signe de la seconde ligne ($L_2 \leftarrow -L_2$) pour faire apparaître 1 au coefficient du pivot (2,2) (deuxième ligne, deuxième colonne) :

$$\left\{\begin{array}{rrrrcrl} x_1 & -2x_2 & +3x_3 & +17x_4 & = & 4 & \\ & x_2 & -2x_3 & -13x_4 & = & -5 & L_2 \leftarrow -L_2 \\ & x_2 & & -3x_4 & = & 3 & \end{array}\right.$$

On fait disparaître le terme x_2 de la troisième ligne, puis on fait apparaître un coefficient 1 pour le pivot de la position (3,3) :

$$\left\{\begin{array}{rrrrcrl} x_1 & -2x_2 & +3x_3 & +17x_4 & = & 4 & \\ & x_2 & -2x_3 & -13x_4 & = & -5 & \\ & & 2x_3 & +10x_4 & = & 8 & L_3 \leftarrow L_3 - L_2 \end{array}\right. \qquad \left\{\begin{array}{rrrrcrl} x_1 & -2x_2 & +3x_3 & +17x_4 & = & 4 & \\ & x_2 & -2x_3 & -13x_4 & = & -5 & \\ & & x_3 & +5x_4 & = & 4 & L_3 \leftarrow \frac{1}{2}L_3 \end{array}\right.$$

Le système est maintenant sous forme échelonnée.

Partie B. Passage à une forme réduite.
Il reste à le mettre sous la forme échelonnée réduite. Pour cela, on ajoute à une ligne des multiples adéquats des lignes situées au-dessous d'elle, en allant du bas à droite vers le haut à gauche.
On fait apparaître des 0 sur la troisième colonne en utilisant le pivot de la troisième ligne :

$$\left\{\begin{array}{rrrrcrl} x_1 & -2x_2 & +3x_3 & +17x_4 & = & 4 & \\ & x_2 & & -3x_4 & = & 3 & L_2 \leftarrow L_2 + 2L_3 \\ & & x_3 & +5x_4 & = & 4 & \end{array}\right. \qquad \left\{\begin{array}{rrrrcrl} x_1 & -2x_2 & & 2x_4 & = & -8 & L_1 \leftarrow L_1 - 3L_3 \\ & x_2 & & -3x_4 & = & 3 & \\ & & x_3 & +5x_4 & = & 4 & \end{array}\right.$$

On fait apparaître des 0 sur la deuxième colonne (en utilisant le pivot de la deuxième ligne) :

$$\left\{\begin{array}{rrrrcrl} x_1 & & & -4x_4 & = & -2 & L_1 \leftarrow L_1 + 2L_2 \\ & x_2 & & -3x_4 & = & 3 & \\ & & x_3 & +5x_4 & = & 4 & \end{array}\right.$$

Le système est sous forme échelonnée réduite.

Partie C. Solutions. Le système est maintenant très simple à résoudre. En choisissant x_4 comme variable libre, on peut exprimer x_1, x_2, x_3 en fonction de x_4 :

$$x_1 = 4x_4 - 2, \quad x_2 = 3x_4 + 3, \quad x_3 = -5x_4 + 4.$$

Ce qui permet d'obtenir toutes les solutions du système :

$$\mathcal{S} = \left\{(4x_4 - 2, 3x_4 + 3, -5x_4 + 4, x_4) \mid x_4 \in \mathbb{R}\right\}.$$

3.4. Systèmes homogènes

Le fait que l'on puisse toujours se ramener à un système échelonné réduit implique le résultat suivant :

Théorème 44

Tout système homogène d'équations linéaires dont le nombre d'inconnues est strictement plus grand que le nombre d'équations a une infinité de solutions.

Exemple 153

Considérons le système homogène

$$\begin{cases} 3x_1 + 3x_2 - 2x_3 - x_5 = 0 \\ -x_1 - x_2 + x_3 + 3x_4 + x_5 = 0 \\ 2x_1 + 2x_2 - x_3 + 2x_4 + 2x_5 = 0 \\ x_3 + 8x_4 + 4x_5 = 0. \end{cases}$$

Sa forme échelonnée réduite est

$$\begin{cases} x_1 + x_2 + 13x_5 = 0 \\ x_3 + 20x_5 = 0 \\ x_4 - 2x_5 = 0. \end{cases}$$

On pose comme variables libres x_2 et x_5 pour avoir

$$x_1 = -x_2 - 13x_5, \qquad x_3 = -20x_5, \qquad x_4 = 2x_5,$$

et l'ensemble des solutions :

$$\mathscr{S} = \{(-x_2 - 13x_5, x_2, -20x_5, 2x_5, x_5) \mid x_2, x_5 \in \mathbb{R}\}$$

qui est bien infini.

Mini-exercices

1. Écrire un système linéaire à 4 équations et 5 inconnues qui soit échelonné mais pas réduit. Idem avec échelonné, non réduit, dont tous les coefficients sont 0 ou +1. Idem avec échelonné et réduit.
2. Résoudre les systèmes échelonnés suivants : $\begin{cases} 2x_1 - x_2 + x_4 = 1 \\ x_2 + x_3 - 2x_4 = 3 \\ 2x_3 + x_4 = 4 \\ x_4 = -2 \end{cases}$

   $\begin{cases} x_1 + x_2 + x_4 = 0 \\ x_2 + x_3 = 0 \\ 2x_3 + x_4 = 0 \end{cases}$ $\qquad \begin{cases} x_1 + 2x_2 + x_4 = 0 \\ 2x_3 - 3x_4 = 0 \end{cases}$
3. Si l'on passe d'un système (S) par une des trois opérations élémentaires à un système (S'), alors quelle opération permet de passer de (S') à (S) ?
4. Résoudre les systèmes linéaires suivants par la méthode du pivot de Gauss :

   $$\begin{cases} 2x + y + z = 3 \\ x - y + 3z = 8 \\ x + 2y - z = -3 \end{cases} \qquad \begin{cases} 2x_1 + 4x_2 - 6x_3 - 2x_4 = 2 \\ 3x_1 + 6x_2 - 7x_3 + 4x_4 = 2 \\ 5x_1 + 10x_2 - 11x_3 + 6x_4 = 3 \end{cases}$$
5. Résoudre le système suivant, selon les valeurs de $a, b \in \mathbb{R}$: $\begin{cases} x + y - z = a \\ -x + 2z = b \\ 2y + 2z = 4 \end{cases}$

Auteurs

- D'après un cours de Eva Bayer-Fluckiger, Philippe Chabloz, Lara Thomas de l'École Polytechnique Fédérale de Lausanne,
- et un cours de Sophie Chemla de l'université Pierre et Marie Curie, reprenant des parties d'un cours de H. Ledret et d'une équipe de l'université de Bordeaux animée par J. Queyrut,
- mixés et révisés par Arnaud Bodin, relu par Vianney Combet.



16 Matrices

Vidéo ■ partie 1. Définition
Vidéo ■ partie 2. Multiplication de matrices
Vidéo ■ partie 3. Inverse d'une matrice : définition
Vidéo ■ partie 4. Inverse d'une matrice : calcul
Vidéo ■ partie 5. Inverse d'une matrice : systèmes linéaires et matrices élémentaires
Vidéo ■ partie 6. Matrices triangulaires, transposition, trace, matrices symétriques

Les matrices sont des tableaux de nombres. La résolution d'un certain nombre de problèmes d'algèbre linéaire se ramène à des manipulations sur les matrices. Ceci est vrai en particulier pour la résolution des systèmes linéaires.

Dans ce chapitre, $\mathbb{K}$ désigne un corps. On peut penser à $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

1. Définition

1.1. Définition

Définition 80

- Une ***matrice*** A est un tableau rectangulaire d'éléments de $\mathbb{K}$.
- Elle est dite de ***taille*** $n \times p$ si le tableau possède n lignes et p colonnes.
- Les nombres du tableau sont appelés les ***coefficients*** de A.
- Le coefficient situé à la i-ème ligne et à la j-ème colonne est noté $a_{i,j}$.

Un tel tableau est représenté de la manière suivante :

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,j} & \dots & a_{1,p} \\ a_{2,1} & a_{2,2} & \dots & a_{2,j} & \dots & a_{2,p} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i,1} & a_{i,2} & \dots & a_{i,j} & \dots & a_{i,p} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n,1} & a_{n,2} & \dots & a_{n,j} & \dots & a_{n,p} \end{pmatrix} \qquad \text{ou} \qquad A = \left(a_{i,j}\right)_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant p}} \qquad \text{ou} \qquad \left(a_{i,j}\right).$$

Exemple 154

$$A = \begin{pmatrix} 1 & -2 & 5 \\ 0 & 3 & 7 \end{pmatrix}$$

est une matrice 2×3 avec, par exemple, $a_{1,1} = 1$ et $a_{2,3} = 7$.

Encore quelques définitions :

Définition 81

- Deux matrices sont ***égales*** lorsqu'elles ont la même taille et que les coefficients correspondants sont égaux.
- L'ensemble des matrices à n lignes et p colonnes à coefficients dans $\mathbb{K}$ est noté $M_{n,p}(\mathbb{K})$. Les éléments de $M_{n,p}(\mathbb{R})$ sont appelés ***matrices réelles***.

1.2. Matrices particulières

Voici quelques types de matrices intéressantes :

- Si $n = p$ (même nombre de lignes que de colonnes), la matrice est dite ***matrice carrée***. On note $M_n(\mathbb{K})$ au lieu de $M_{n,n}(\mathbb{K})$.

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix}$$

  Les éléments $a_{1,1}, a_{2,2}, \dots, a_{n,n}$ forment la ***diagonale principale*** de la matrice.
- Une matrice qui n'a qu'une seule ligne ($n = 1$) est appelée ***matrice ligne*** ou ***vecteur ligne***. On la note

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,p} \end{pmatrix}.$$

- De même, une matrice qui n'a qu'une seule colonne ($p = 1$) est appelée ***matrice colonne*** ou ***vecteur colonne***. On la note

$$A = \begin{pmatrix} a_{1,1} \\ a_{2,1} \\ \vdots \\ a_{n,1} \end{pmatrix}.$$

- La matrice (de taille $n \times p$) dont tous les coefficients sont des zéros est appelée la ***matrice nulle*** et est notée $0_{n,p}$ ou plus simplement 0. Dans le calcul matriciel, la matrice nulle joue le rôle du nombre 0 pour les réels.

1.3. Addition de matrices

Définition 82. Somme de deux matrices

Soient A et B deux matrices ayant la même taille $n \times p$. Leur ***somme*** $C = A + B$ est la matrice de taille $n \times p$ définie par

$$c_{ij} = a_{ij} + b_{ij}.$$

En d'autres termes, on somme coefficients par coefficients. Remarque : on note indifféremment a_{ij} où $a_{i,j}$ pour les coefficients de la matrice A.

Exemple 155

$$\text{Si}\quad A=\begin{pmatrix}3&-2\\1&7\end{pmatrix}\quad\text{et}\quad B=\begin{pmatrix}0&5\\2&-1\end{pmatrix}\quad\text{alors}\quad A+B=\begin{pmatrix}3&3\\3&6\end{pmatrix}.$$

$$\text{Par contre si}\quad B'=\begin{pmatrix}-2\\8\end{pmatrix}\quad\text{alors}\quad A+B'\quad\text{n'est pas définie.}$$

Définition 83. Produit d'une matrice par un scalaire

Le produit d'une matrice $A=(a_{ij})$ de $M_{n,p}(\mathbb{K})$ par un scalaire $\alpha\in\mathbb{K}$ est la matrice (αa_{ij}) formée en multipliant chaque coefficient de A par α. Elle est notée $\alpha\cdot A$ (ou simplement αA).

Exemple 156

$$\text{Si}\quad A=\begin{pmatrix}1&2&3\\0&1&0\end{pmatrix}\quad\text{et}\quad\alpha=2\quad\text{alors}\quad\alpha A=\begin{pmatrix}2&4&6\\0&2&0\end{pmatrix}.$$

La matrice $(-1)A$ est l'***opposée*** de A et est notée $-A$. La ***différence*** $A-B$ est définie par $A+(-B)$.

Exemple 157

$$\text{Si}\quad A=\begin{pmatrix}2&-1&0\\4&-5&2\end{pmatrix}\quad\text{et}\quad B=\begin{pmatrix}-1&4&2\\7&-5&3\end{pmatrix}\quad\text{alors}\quad A-B=\begin{pmatrix}3&-5&-2\\-3&0&-1\end{pmatrix}.$$

L'addition et la multiplication par un scalaire se comportent sans surprises :

Proposition 98

Soient A, B et C trois matrices appartenant à $M_{n,p}(\mathbb{K})$. Soient $\alpha\in\mathbb{K}$ et $\beta\in\mathbb{K}$ deux scalaires.

1. $A+B=B+A$: la somme est commutative,
2. $A+(B+C)=(A+B)+C$: la somme est associative,
3. $A+0=A$: la matrice nulle est l'élément neutre de l'addition,
4. $(\alpha+\beta)A=\alpha A+\beta A$,
5. $\alpha(A+B)=\alpha A+\alpha B$.

Démonstration

Prouvons par exemple le quatrième point. Le terme général de $(\alpha+\beta)A$ est égal à $(\alpha+\beta)a_{ij}$. D'après les règles de calcul dans $\mathbb{K}$, $(\alpha+\beta)a_{ij}$ est égal à $\alpha a_{ij}+\beta a_{ij}$ qui est le terme général de la matrice $\alpha A+\beta A$.

Mini-exercices

1. Soient $A=\begin{pmatrix}-7&2\\0&-1\\1&-4\end{pmatrix}$, $B=\begin{pmatrix}1&2&3\\2&3&1\\3&2&1\end{pmatrix}$, $C=\begin{pmatrix}21&-6\\0&3\\-3&12\end{pmatrix}$, $D=\frac{1}{2}\begin{pmatrix}1&0&1\\0&1&0\\1&1&1\end{pmatrix}$, $E=\begin{pmatrix}1&2\\-3&0\\-8&6\end{pmatrix}$. Calculer toutes les sommes possibles de deux de ces matrices. Calculer $3A+2C$ et $5B-4D$. Trouver α tel que $A-\alpha C$ soit la matrice nulle.

2. Montrer que si $A+B=A$, alors B est la matrice nulle.
3. Que vaut $0\cdot A$? et $1\cdot A$? Justifier l'affirmation : $\alpha(\beta A)=(\alpha\beta)A$. Idem avec $nA = A+A+\cdots+A$ (n occurrences de A).

2. Multiplication de matrices

2.1. Définition du produit

Le produit AB de deux matrices A et B est défini si et seulement si le nombre de colonnes de A est égal au nombre de lignes de B.

Définition 84. Produit de deux matrices

Soient $A=(a_{ij})$ une matrice $n\times p$ et $B=(b_{ij})$ une matrice $p\times q$. Alors le produit $C=AB$ est une matrice $n\times q$ dont les coefficients c_{ij} sont définis par :

$$\boxed{c_{ij}=\sum_{k=1}^{p} a_{ik}b_{kj}}$$

On peut écrire le coefficient de façon plus développée, à savoir :

$$c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{ik}b_{kj}+\cdots+a_{ip}b_{pj}.$$

Il est commode de disposer les calculs de la façon suivante.

$$\begin{array}{ccc} & \begin{pmatrix} & & & \times & & \\ & & & \times & & \\ & & & \times & & \\ & & & \times & & \end{pmatrix} & \leftarrow B \\ A\rightarrow \begin{pmatrix} \\ \times & \times & \times & \times \\ \end{pmatrix} & \begin{pmatrix} & & & | & & \\ & & & | & & \\ - & - & - & c_{ij} & & \end{pmatrix} & \leftarrow AB \end{array}$$

Avec cette disposition, on considère d'abord la ligne de la matrice A située à gauche du coefficient que l'on veut calculer (ligne représentée par des $\times$ dans A) et aussi la colonne de la matrice B située au-dessus du coefficient que l'on veut calculer (colonne représentée par des $\times$ dans B). On calcule le produit du premier coefficient de la ligne par le premier coefficient de la colonne ($a_{i1}\times b_{1j}$), que l'on ajoute au produit du deuxième coefficient de la ligne par le deuxième coefficient de la colonne ($a_{i2}\times b_{2j}$), que l'on ajoute au produit du troisième...

2.2. Exemples

Exemple 158

$$A=\begin{pmatrix}1&2&3\\2&3&4\end{pmatrix}\qquad B=\begin{pmatrix}1&2\\-1&1\\1&1\end{pmatrix}$$

On dispose d'abord le produit correctement (à gauche) : la matrice obtenue est de taille 2×2. Puis on calcule chacun des coefficients, en commençant par le premier coefficient $c_{11} = 1\times 1\ +\ 2\times(-1)\ +\ 3\times 1 = 2$ (au milieu), puis les autres (à droite).

$$\begin{pmatrix}1&2&3\\2&3&4\end{pmatrix}\begin{pmatrix}1&2\\-1&1\\1&1\end{pmatrix} \qquad \begin{pmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{pmatrix} \qquad\qquad \begin{pmatrix}1&2&3\\2&3&4\end{pmatrix}\begin{pmatrix}1&2\\-1&1\\1&1\end{pmatrix} \qquad \begin{pmatrix}2&c_{12}\\c_{21}&c_{22}\end{pmatrix} \qquad\qquad \begin{pmatrix}1&2&3\\2&3&4\end{pmatrix}\begin{pmatrix}1&2\\-1&1\\1&1\end{pmatrix} \qquad \begin{pmatrix}2&7\\3&11\end{pmatrix}$$

Un exemple intéressant est le produit d'un vecteur ligne par un vecteur colonne :

$$u = \begin{pmatrix}a_1 & a_2 & \cdots & a_n\end{pmatrix} \qquad v = \begin{pmatrix}b_1\\b_2\\\vdots\\b_n\end{pmatrix}$$

Alors $u \times v$ est une matrice de taille 1×1 dont l'unique coefficient est $a_1b_1 + a_2b_2 + \cdots + a_nb_n$. Ce nombre s'appelle le ***produit scalaire*** des vecteurs u et v.

Calculer le coefficient c_{ij} dans le produit $A \times B$ revient donc à calculer le produit scalaire des vecteurs formés par la i-ème ligne de A et la j-ème colonne de B.

2.3. Pièges à éviter

Premier piège. Le produit de matrices n'est pas commutatif en général.
En effet, il se peut que AB soit défini mais pas BA, ou que AB et BA soient tous deux définis mais pas de la même taille. Mais même dans le cas où AB et BA sont définis et de la même taille, on a en général $AB \neq BA$.

Exemple 159

$$\begin{pmatrix}5&1\\3&-2\end{pmatrix}\begin{pmatrix}2&0\\4&3\end{pmatrix} = \begin{pmatrix}14&3\\-2&-6\end{pmatrix} \qquad \text{mais} \qquad \begin{pmatrix}2&0\\4&3\end{pmatrix}\begin{pmatrix}5&1\\3&-2\end{pmatrix} = \begin{pmatrix}10&2\\29&-2\end{pmatrix}.$$

Deuxième piège. $AB = 0$ n'implique pas $A = 0$ ou $B = 0$.
Il peut arriver que le produit de deux matrices non nulles soit nul. En d'autres termes, on peut avoir $A \neq 0$ et $B \neq 0$ mais $AB = 0$.

Exemple 160

$$A = \begin{pmatrix}0&-1\\0&5\end{pmatrix} \qquad B = \begin{pmatrix}2&-3\\0&0\end{pmatrix} \qquad \text{et} \qquad AB = \begin{pmatrix}0&0\\0&0\end{pmatrix}.$$

Troisième piège. $AB = AC$ n'implique pas $B = C$. On peut avoir $AB = AC$ et $B \neq C$.

Exemple 161

$$A = \begin{pmatrix}0&-1\\0&3\end{pmatrix} \qquad B = \begin{pmatrix}4&-1\\5&4\end{pmatrix} \qquad C = \begin{pmatrix}2&5\\5&4\end{pmatrix} \qquad \text{et} \qquad AB = AC = \begin{pmatrix}-5&-4\\15&12\end{pmatrix}.$$

2.4. Propriétés du produit de matrices

Malgré les difficultés soulevées au-dessus, le produit vérifie les propriétés suivantes :

Proposition 99

1. $A(BC) = (AB)C$: associativité du produit,
2. $A(B+C) = AB + AC$ et $(B+C)A = BA + CA$: distributivité du produit par rapport à la somme,
3. $A \cdot 0 = 0$ et $0 \cdot A = 0$.

Démonstration

Posons $A = (a_{ij}) \in M_{n,p}(\mathbb{K})$, $B = (b_{ij}) \in M_{p,q}(\mathbb{K})$ et $C = (c_{ij}) \in M_{q,r}(\mathbb{K})$. Prouvons que $A(BC) = (AB)C$ en montrant que les matrices $A(BC)$ et $(AB)C$ ont les mêmes coefficients.

Le terme d'indice (i,k) de la matrice AB est $x_{ik} = \sum_{\ell=1}^{p} a_{i\ell} b_{\ell k}$. Le terme d'indice (i,j) de la matrice $(AB)C$ est donc

$$\sum_{k=1}^{q} x_{ik} c_{kj} = \sum_{k=1}^{q} \left(\sum_{\ell=1}^{p} a_{i\ell} b_{\ell k} \right) c_{kj}.$$

Le terme d'indice (ℓ,j) de la matrice BC est $y_{\ell j} = \sum_{k=1}^{q} b_{\ell k} c_{kj}$. Le terme d'indice (i,j) de la matrice $A(BC)$ est donc

$$\sum_{\ell=1}^{p} a_{i\ell} \left(\sum_{k=1}^{q} b_{\ell k} c_{kj} \right).$$

Comme dans $\mathbb{K}$ la multiplication est distributive et associative, les coefficients de $(AB)C$ et $A(BC)$ coïncident. Les autres démonstrations se font comme celle de l'associativité.

2.5. La matrice identité

La matrice carrée suivante s'appelle ***la matrice identité*** :

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Ses éléments diagonaux sont égaux à 1 et tous ses autres éléments sont égaux à 0. Elle se note I_n ou simplement I. Dans le calcul matriciel, la matrice identité joue un rôle analogue à celui du nombre 1 pour les réels. C'est l'élément neutre pour la multiplication. En d'autres termes :

Proposition 100

Si A est une matrice $n \times p$, alors

$$I_n \cdot A = A \qquad \text{et} \qquad A \cdot I_p = A.$$

Démonstration

Nous allons détailler la preuve. Soit $A \in M_{n,p}(\mathbb{K})$ de terme général a_{ij}. La matrice unité d'ordre p est telle que tous les éléments de la diagonale principale sont égaux à 1, les autres étant tous nuls. On peut formaliser cela en introduisant le symbole de Kronecker. Si i et j sont deux entiers, on appelle ***symbole de Kronecker***, et on note $\delta_{i,j}$, le réel qui vaut 0 si i est différent de j, et 1 si i est égal à j. Donc

$$\delta_{i,j} = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j. \end{cases}$$

Alors le terme général de la matrice identité I_p est $\delta_{i,j}$ avec i et j entiers, compris entre 1 et p.
La matrice produit AI_p est une matrice appartenant à $M_{n,p}(\mathbb{K})$ dont le terme général c_{ij} est donné par la formule $c_{ij} = \sum_{k=1}^{p} a_{ik}\delta_{kj}$. Dans cette somme, i et j sont fixés et k prend toutes les valeurs comprises entre 1 et p. Si $k \neq j$ alors $\delta_{kj} = 0$, et si $k = j$ alors $\delta_{kj} = 1$. Donc dans la somme qui définit c_{ij}, tous les termes correspondant à des valeurs de k différentes de j sont nuls et il reste donc $c_{ij} = a_{ij}\delta_{jj} = a_{ij}1 = a_{ij}$. Donc les matrices AI_p et A ont le même terme général et sont donc égales. L'égalité $I_nA = A$ se démontre de la même façon.

2.6. Puissance d'une matrice

Dans l'ensemble $M_n(\mathbb{K})$ des matrices carrées de taille $n \times n$ à coefficients dans $\mathbb{K}$, la multiplication des matrices est une opération interne : si $A, B \in M_n(\mathbb{K})$ alors $AB \in M_n(\mathbb{K})$.
En particulier, on peut multiplier une matrice carrée par elle-même : on note $A^2 = A \times A$, $A^3 = A \times A \times A$.
On peut ainsi définir les puissances successives d'une matrice :

Définition 85

Pour tout $A \in M_n(\mathbb{K})$, on définit les puissances successives de A par $A^0 = I_n$ et $A^{p+1} = A^p \times A$ pour tout $p \in \mathbb{N}$. Autrement dit, $A^p = \underbrace{A \times A \times \cdots \times A}_{p \text{ facteurs}}$.

Exemple 162

On cherche à calculer A^p avec $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. On calcule A^2, A^3 et A^4 et on obtient :

$$A^2 = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix} \qquad A^3 = A^2 \times A = \begin{pmatrix} 1 & 0 & 7 \\ 0 & -1 & 0 \\ 0 & 0 & 8 \end{pmatrix} \qquad A^4 = A^3 \times A = \begin{pmatrix} 1 & 0 & 15 \\ 0 & 1 & 0 \\ 0 & 0 & 16 \end{pmatrix}.$$

L'observation de ces premières puissances permet de penser que la formule est : $A^p = \begin{pmatrix} 1 & 0 & 2^p - 1 \\ 0 & (-1)^p & 0 \\ 0 & 0 & 2^p \end{pmatrix}$. Démontrons ce résultat par récurrence.
Il est vrai pour $p = 0$ (on trouve l'identité). On le suppose vrai pour un entier p et on va le démontrer pour $p+1$. On a, d'après la définition,

$$A^{p+1} = A^p \times A = \begin{pmatrix} 1 & 0 & 2^p - 1 \\ 0 & (-1)^p & 0 \\ 0 & 0 & 2^p \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2^{p+1} - 1 \\ 0 & (-1)^{p+1} & 0 \\ 0 & 0 & 2^{p+1} \end{pmatrix}.$$

Donc la propriété est démontrée.

2.7. Formule du binôme

Comme la multiplication n'est pas commutative, les identités binomiales usuelles sont fausses. En particulier, $(A+B)^2$ ne vaut en général pas $A^2+2AB+B^2$, mais on sait seulement que

$$(A+B)^2 = A^2 + AB + BA + B^2.$$

Proposition 101. Calcul de $(A+B)^p$ lorsque $AB = BA$

Soient A et B deux éléments de $M_n(\mathbb{K})$ qui ***commutent***, c'est-à-dire tels que $AB = BA$. Alors, pour tout entier $p \geqslant 0$, on a la formule

$$(A+B)^p = \sum_{k=0}^{p} \binom{p}{k} A^{p-k} B^k$$

où $\binom{p}{k}$ désigne le coefficient du binôme.

La démonstration est similaire à celle de la formule du binôme pour $(a+b)^p$, avec $a, b \in \mathbb{R}$.

Exemple 163

Soit $A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. On pose $N = A - I = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. La matrice N est nilpotente (c'est-à-dire il existe $k \in \mathbb{N}$ tel que $N^k = 0$) comme le montrent les calculs suivants :

$$N^2 = \begin{pmatrix} 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad N^3 = \begin{pmatrix} 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \text{et} \qquad N^4 = 0.$$

Comme on a $A = I + N$ et les matrices N et I commutent (la matrice identité commute avec toutes les matrices), on peut appliquer la formule du binôme de Newton. On utilise que $I^k = I$ pour tout k et surtout que $N^k = 0$ si $k \geqslant 4$. On obtient

$$A^p = \sum_{k=0}^{p} \binom{p}{k} N^k I^{p-k} = \sum_{k=0}^{3} \binom{p}{k} N^k = I + pN + \tfrac{p(p-1)}{2!} N^2 + \tfrac{p(p-1)(p-2)}{3!} N^3.$$

D'où

$$A^p = \begin{pmatrix} 1 & p & p^2 & p(p^2-p+1) \\ 0 & 1 & 2p & p(3p-2) \\ 0 & 0 & 1 & 3p \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Mini-exercices

1. Soient $A=\begin{pmatrix} 0 & 2 & -2 \\ 6 & -4 & 0 \end{pmatrix}$, $B=\begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 0 \\ 2 & -2 & -3 \end{pmatrix}$, $C=\begin{pmatrix} 8 & 2 \\ -3 & 2 \\ -5 & 5 \end{pmatrix}$, $D=\begin{pmatrix} 5 \\ 2 \\ -1 \end{pmatrix}$, $E=\begin{pmatrix} x & y & z \end{pmatrix}$. Quels produits sont possibles ? Les calculer !
2. Soient $A=\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{pmatrix}$ et $B=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 1 & -1 & 0 \end{pmatrix}$. Calculer A^2, B^2, AB et BA.
3. Soient $A=\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ et $B=\begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 3 & 1 & 0 \end{pmatrix}$. Calculer A^p et B^p pour tout $p \geqslant 0$. Montrer que $AB=BA$. Calculer $(A+B)^p$.

3. Inverse d'une matrice : définition

3.1. Définition

Définition 86. Matrice inverse

Soit A une matrice carrée de taille $n \times n$. S'il existe une matrice carrée B de taille $n \times n$ telle que

$$AB = I \qquad \text{et} \qquad BA = I,$$

on dit que A est ***inversible***. On appelle B l'***inverse de A*** et on la note A^{-1}.

On verra plus tard qu'il suffit en fait de vérifier une seule des conditions $AB = I$ ou bien $BA = I$.

- Plus généralement, quand A est inversible, pour tout $p \in \mathbb{N}$, on note :

$$A^{-p} = (A^{-1})^p = \underbrace{A^{-1}A^{-1}\cdots A^{-1}}_{p \text{ facteurs}}.$$

- L'ensemble des matrices inversibles de $M_n(\mathbb{K})$ est noté $GL_n(\mathbb{K})$.

3.2. Exemples

Exemple 164

Soit $A=\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$. Étudier si A est inversible, c'est étudier l'existence d'une matrice $B=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients dans $\mathbb{K}$, telle que $AB = I$ et $BA = I$. Or $AB = I$ équivaut à :

$$AB = I \iff \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \iff \begin{pmatrix} a+2c & b+2d \\ 3c & 3d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Cette égalité équivaut au système :

$$\begin{cases} a+2c=1 \\ b+2d=0 \\ 3c=0 \\ 3d=1 \end{cases}$$

Sa résolution est immédiate : $a=1$, $b=-\frac{2}{3}$, $c=0$, $d=\frac{1}{3}$. Il n'y a donc qu'une seule matrice possible, à savoir $B=\begin{pmatrix} 1 & -\frac{2}{3} \\ 0 & \frac{1}{3} \end{pmatrix}$. Pour prouver qu'elle convient, il faut aussi montrer l'égalité $BA = I$, dont la vérification est laissée au lecteur. La matrice A est donc inversible et $A^{-1} =$

$\begin{pmatrix} 1 & -\frac{2}{3} \\ 0 & \frac{1}{3} \end{pmatrix}$.

Exemple 165

La matrice $A = \left(\begin{smallmatrix} 3 & 0 \\ 5 & 0 \end{smallmatrix}\right)$ n'est pas inversible. En effet, soit $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice quelconque. Alors le produit

$$BA = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 5 & 0 \end{pmatrix} = \begin{pmatrix} 3a+5b & 0 \\ 3c+5d & 0 \end{pmatrix}$$

ne peut jamais être égal à la matrice identité.

Exemple 166

- Soit I_n la matrice carrée identité de taille $n \times n$. C'est une matrice inversible, et son inverse est elle-même par l'égalité $I_n I_n = I_n$.
- La matrice nulle 0_n de taille $n \times n$ n'est pas inversible. En effet on sait que, pour toute matrice B de $M_n(\mathbb{K})$, on a $B0_n = 0_n$, qui ne peut jamais être la matrice identité.

3.3. Propriétés

Unicité

Proposition 102

Si A est inversible, alors son inverse est unique.

Démonstration

La méthode classique pour mener à bien une telle démonstration est de supposer l'existence de deux matrices B_1 et B_2 satisfaisant aux conditions imposées et de démontrer que $B_1 = B_2$.
Soient donc B_1 telle que $AB_1 = B_1A = I_n$ et B_2 telle que $AB_2 = B_2A = I_n$. Calculons $B_2(AB_1)$. D'une part, comme $AB_1 = I_n$, on a $B_2(AB_1) = B_2$. D'autre part, comme le produit des matrices est associatif, on a $B_2(AB_1) = (B_2A)B_1 = I_nB_1 = B_1$. Donc $B_1 = B_2$.

Inverse de l'inverse

Proposition 103

Soit A une matrice inversible. Alors A^{-1} est aussi inversible et on a :

$$\boxed{(A^{-1})^{-1} = A}$$

Inverse d'un produit

Proposition 104

Soient A et B deux matrices inversibles de même taille. Alors AB est inversible et

$$\boxed{(AB)^{-1} = B^{-1}A^{-1}}$$

Il faut bien faire attention à l'inversion de l'ordre !

Démonstration

Il suffit de montrer $(B^{-1}A^{-1})(AB) = I$ et $(AB)(B^{-1}A^{-1}) = I$. Cela suit de

$$\begin{aligned} & (B^{-1}A^{-1})(AB) = B^{-1}(AA^{-1})B = B^{-1}IB = B^{-1}B = I, \\ \text{et} \quad & (AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I. \end{aligned}$$

De façon analogue, on montre que si $A_1, \ldots, A_m$ sont inversibles, alors

$$(A_1A_2 \cdots A_m)^{-1} = A_m^{-1}A_{m-1}^{-1} \cdots A_1^{-1}.$$

Simplification par une matrice inversible

Si C est une matrice quelconque de $M_n(\mathbb{K})$, nous avons vu que la relation $AC = BC$ où A et B sont des éléments de $M_n(\mathbb{K})$ n'entraîne pas forcément l'égalité $A = B$. En revanche, si C est une matrice inversible, on a la proposition suivante :

Proposition 105

Soient A et B deux matrices de $M_n(\mathbb{K})$ et C une matrice inversible de $M_n(\mathbb{K})$. Alors l'égalité $AC = BC$ implique l'égalité $A = B$.

Démonstration

Ce résultat est immédiat : si on multiplie à droite l'égalité $AC = BC$ par C^{-1}, on obtient l'égalité : $(AC)C^{-1} = (BC)C^{-1}$. En utilisant l'associativité du produit des matrices on a $A(CC^{-1}) = B(CC^{-1})$, ce qui donne d'après la définition de l'inverse $AI = BI$, d'où $A = B$.

Mini-exercices

1. Soient $A = \begin{pmatrix} -1 & -2 \\ 3 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}$. Calculer A^{-1}, B^{-1} , $(AB)^{-1}$, $(BA)^{-1}$, A^{-2}.
2. Calculer l'inverse de $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix}$.
3. Soit $A = \begin{pmatrix} -1 & -2 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Calculer $2A - A^2$. Sans calculs, en déduire A^{-1}.

4. Inverse d'une matrice : calcul

Nous allons voir une méthode pour calculer l'inverse d'une matrice quelconque de manière efficace. Cette méthode est une reformulation de la méthode du pivot de Gauss pour les systèmes linéaires. Auparavant, nous commençons par une formule directe dans le cas simple des matrices 2×2.

4.1. Matrices 2×2

Considérons la matrice 2×2 : $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Proposition 106

Si $ad - bc \neq 0$, alors A est inversible et

$$A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Démonstration

On vérifie que si $B = \frac{1}{ad-bc}\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ alors $AB = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Idem pour BA.

4.2. Méthode de Gauss pour inverser les matrices

La méthode pour inverser une matrice A consiste à faire des opérations élémentaires sur les lignes de la matrice A jusqu'à la transformer en la matrice identité I. On fait simultanément les mêmes opérations élémentaires en partant de la matrice I. On aboutit alors à une matrice qui est A^{-1}. La preuve sera vue dans la section suivante.

En pratique, on fait les deux opérations en même temps en adoptant la disposition suivante : à côté de la matrice A que l'on veut inverser, on rajoute la matrice identité pour former un tableau $(A \mid I)$. Sur les lignes de cette matrice augmentée, on effectue des opérations élémentaires jusqu'à obtenir le tableau $(I \mid B)$. Et alors $B = A^{-1}$.

Ces opérations élémentaires sur les lignes sont :

1. $L_i \leftarrow \lambda L_i$ avec $\lambda \neq 0$: on peut multiplier une ligne par un réel non nul (ou un élément de $\mathbb{K}\setminus\{0\}$).
2. $L_i \leftarrow L_i + \lambda L_j$ avec $\lambda \in \mathbb{K}$ (et $j \neq i$) : on peut ajouter à la ligne L_i un multiple d'une autre ligne L_j.
3. $L_i \leftrightarrow L_j$: on peut échanger deux lignes.

N'oubliez pas : tout ce que vous faites sur la partie gauche de la matrice augmentée, vous devez aussi le faire sur la partie droite.

4.3. Un exemple

Calculons l'inverse de $A = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 0 & -1 \\ -1 & 2 & 2 \end{pmatrix}$.

Voici la matrice augmentée, avec les lignes numérotées :

$$(A \mid I) = \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 4 & 0 & -1 & 0 & 1 & 0 \\ -1 & 2 & 2 & 0 & 0 & 1 \end{array}\right) \begin{array}{l} L_1 \\ L_2 \\ L_3 \end{array}$$

On applique la méthode de Gauss pour faire apparaître des 0 sur la première colonne, d'abord sur la deuxième ligne par l'opération élémentaire $L_2 \leftarrow L_2 - 4L_1$ qui conduit à la matrice augmentée :

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & -8 & -5 & -4 & 1 & 0 \\ -1 & 2 & 2 & 0 & 0 & 1 \end{array}\right) {\scriptstyle L_2 \leftarrow L_2 - 4L_1}$$

Puis un 0 sur la première colonne, à la troisième ligne, avec $L_3 \leftarrow L_3 + L_1$:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & -8 & -5 & -4 & 1 & 0 \\ 0 & 4 & 3 & 1 & 0 & 1 \end{array}\right) {\scriptstyle L_3 \leftarrow L_3 + L_1}$$

On multiplie la ligne L_2 afin qu'elle commence par 1 :

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & \frac{5}{8} & \frac{1}{2} & -\frac{1}{8} & 0 \\ 0 & 4 & 3 & 1 & 0 & 1 \end{array}\right) {\scriptstyle L_2 \leftarrow -\frac{1}{8} L_2}$$

On continue afin de faire apparaître des 0 partout sous la diagonale, et on multiplie la ligne L_3. Ce qui termine la première partie de la méthode de Gauss :

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & \frac{5}{8} & \frac{1}{2} & -\frac{1}{8} & 0 \\ 0 & 0 & \frac{1}{2} & -1 & \frac{1}{2} & 1 \end{array}\right) {\scriptstyle L_3 \leftarrow L_3 - 4L_2} \qquad \text{puis} \qquad \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & \frac{5}{8} & \frac{1}{2} & -\frac{1}{8} & 0 \\ 0 & 0 & 1 & -2 & 1 & 2 \end{array}\right) {\scriptstyle L_3 \leftarrow 2L_3}$$

Il ne reste plus qu'à « remonter » pour faire apparaître des zéros au-dessus de la diagonale :

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & \frac{7}{4} & -\frac{3}{4} & -\frac{5}{4} \\ 0 & 0 & 1 & -2 & 1 & 2 \end{array}\right) {\scriptstyle L_2 \leftarrow L_2 - \frac{5}{8} L_3} \qquad \text{puis} \qquad \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & \frac{7}{4} & -\frac{3}{4} & -\frac{5}{4} \\ 0 & 0 & 1 & -2 & 1 & 2 \end{array}\right) {\scriptstyle L_1 \leftarrow L_1 - 2L_2 - L_3}$$

Ainsi l'inverse de A est la matrice obtenue à droite et après avoir factorisé tous les coefficients par $\frac{1}{4}$, on a obtenu :

$$A^{-1} = \frac{1}{4}\begin{pmatrix} -2 & 2 & 2 \\ 7 & -3 & -5 \\ -8 & 4 & 8 \end{pmatrix}$$

Pour se rassurer sur ses calculs, on n'oublie pas de vérifier rapidement que $A \times A^{-1} = I$.

Mini-exercices

1. Si possible calculer l'inverse des matrices : $\begin{pmatrix} 3 & 1 \\ 7 & 2 \end{pmatrix}$, $\begin{pmatrix} 2 & -3 \\ -5 & 4 \end{pmatrix}$, $\begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}$, $\begin{pmatrix} \alpha+1 & 1 \\ 2 & \alpha \end{pmatrix}$.
2. Soit $A(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Calculer $A(\theta)^{-1}$.
3. Calculer l'inverse des matrices : $\begin{pmatrix} 1 & 3 & 0 \\ 2 & 1 & -1 \\ -2 & 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 2 & -2 & 1 \\ 3 & 0 & 5 \\ 1 & 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 2 & -2 & 0 \\ -1 & 2 & 0 & 1 \\ 0 & 2 & 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ -1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 5 & 3 \end{pmatrix}$.

5. Inverse d'une matrice : systèmes linéaires et matrices élémentaires

5.1. Matrices et systèmes linéaires

Le système linéaire

$$\begin{cases} a_{11}\,x_1 & + & a_{12}\,x_2 & + & \cdots & + & a_{1p}\,x_p & = & b_1 \\ a_{21}\,x_1 & + & a_{22}\,x_2 & + & \cdots & + & a_{2p}\,x_p & = & b_2 \\ & & & & \ldots & & & & \\ a_{n1}\,x_1 & + & a_{n2}\,x_2 & + & \cdots & + & a_{np}\,x_p & = & b_n \end{cases}$$

peut s'écrire sous forme matricielle :

$$\underbrace{\begin{pmatrix} a_{11} & \ldots & a_{1p} \\ a_{21} & \ldots & a_{2p} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{np} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \end{pmatrix}}_{X} = \underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}}_{B}.$$

On appelle $A \in M_{n,p}(\mathbb{K})$ la matrice des coefficients du système. $B \in M_{n,1}(\mathbb{K})$ est le vecteur du second membre. Le vecteur $X \in M_{p,1}(\mathbb{K})$ est une solution du système si et seulement si

$$AX = B.$$

Nous savons que :

Théorème 45

Un système d'équations linéaires n'a soit aucune solution, soit une seule solution, soit une infinité de solutions.

5.2. Matrices inversibles et systèmes linéaires

Considérons le cas où le nombre d'équations égale le nombre d'inconnues :

$$\underbrace{\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{X} = \underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}}_{B}.$$

Alors $A \in M_n(\mathbb{K})$ est une matrice carrée et B un vecteur de $M_{n,1}(\mathbb{K})$. Pour tout second membre, nous pouvons utiliser les matrices pour trouver la solution du système linéaire.

Proposition 107

Si la matrice A est inversible, alors la solution du système $AX = B$ est unique et est :

$$\boxed{X = A^{-1}B.}$$

La preuve est juste de vérifier que si $X = A^{-1}B$, alors $AX = A(A^{-1}B) = (AA^{-1})B = I \cdot B = B$. Réciproquement si $AX = B$, alors nécessairement $X = A^{-1}B$. Nous verrons bientôt que si la matrice n'est pas inversible, alors soit il n'y a pas de solution, soit une infinité.

5.3. Les matrices élémentaires

Pour calculer l'inverse d'une matrice A, et aussi pour résoudre des systèmes linéaires, nous avons utilisé trois opérations élémentaires sur les lignes qui sont :

1. $L_i \leftarrow \lambda L_i$ avec $\lambda \neq 0$: on peut multiplier une ligne par un réel non nul (ou un élément de $\mathbb{K} \setminus \{0\}$).
2. $L_i \leftarrow L_i + \lambda L_j$ avec $\lambda \in \mathbb{K}$ (et $j \neq i$) : on peut ajouter à la ligne L_i un multiple d'une autre ligne L_j.
3. $L_i \leftrightarrow L_j$: on peut échanger deux lignes.

Nous allons définir trois matrices élémentaires $E_{L_i \leftarrow \lambda L_i}$, $E_{L_i \leftarrow L_i + \lambda L_j}$, $E_{L_i \leftrightarrow L_j}$ correspondant à ces opérations. Plus précisément, le produit $E \times A$ correspondra à l'opération élémentaire sur A. Voici les définitions accompagnées d'exemples.

1. La matrice $E_{L_i \leftarrow \lambda L_i}$ est la matrice obtenue en multipliant par λ la i-ème ligne de la matrice identité I_n, où λ est un nombre réel non nul.

$$E_{L_2 \leftarrow 5L_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

2. La matrice $E_{L_i \leftarrow L_i + \lambda L_j}$ est la matrice obtenue en ajoutant λ fois la j-ème ligne de I_n à la i-ème ligne de I_n.

$$E_{L_2 \leftarrow L_2 - 3L_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

3. La matrice $E_{L_i \leftrightarrow L_j}$ est la matrice obtenue en permutant les i-ème et j-ème lignes de I_n.

$$E_{L_2 \leftrightarrow L_4} = E_{L_4 \leftrightarrow L_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Les opérations élémentaires sur les lignes sont réversibles, ce qui entraîne l'inversibilité des matrices élémentaires.

Le résultat de la multiplication d'un matrice élémentaire E par A est la matrice obtenue en effectuant l'opération élémentaire correspondante sur A. Ainsi :

1. La matrice $E_{L_i \leftarrow \lambda L_i} \times A$ est la matrice obtenue en multipliant par λ la i-ème ligne de A.
2. La matrice $E_{L_i \leftarrow L_i + \lambda L_j} \times A$ est la matrice obtenue en ajoutant λ fois la j-ème ligne de A à la i-ème ligne de A.
3. La matrice $E_{L_i \leftrightarrow L_j} \times A$ est la matrice obtenue en permutant les i-ème et j-ème lignes de A.

Exemple 167

1.
$$E_{L_2 \leftarrow \frac{1}{3}L_2} \times A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ \frac{1}{3}y_1 & \frac{1}{3}y_2 & \frac{1}{3}y_3 \\ z_1 & z_2 & z_3 \end{pmatrix}$$

2.
$$E_{L_1 \leftarrow L_1 - 7L_3} \times A = \begin{pmatrix} 1 & 0 & -7 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix} = \begin{pmatrix} x_1 - 7z_1 & x_2 - 7z_2 & x_3 - 7z_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix}$$

3.
$$E_{L_2 \leftrightarrow L_3} \times A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ z_1 & z_2 & z_3 \\ y_1 & y_2 & y_3 \end{pmatrix}$$

5.4. Équivalence à une matrice échelonnée

Définition 87

Deux matrices A et B sont dites ***équivalentes par lignes*** si l'une peut être obtenue à partir de l'autre par une suite d'opérations élémentaires sur les lignes. On note $A \sim B$.

Définition 88

Une matrice est ***échelonnée*** si :

- le nombre de zéros commençant une ligne croît strictement ligne par ligne jusqu'à ce qu'il ne reste plus que des zéros.

Elle est ***échelonnée réduite*** si en plus :

- le premier coefficient non nul d'une ligne (non nulle) vaut 1 ;
- et c'est le seul élément non nul de sa colonne.

Exemple d'une matrice échelonnée (à gauche) et échelonnée réduite (à droite) ; les $*$ désignent des coefficients quelconques, les $+$ des coefficients non nuls :

$$\begin{pmatrix} + & * & * & * & * & * & * \\ 0 & 0 & + & * & * & * & * \\ 0 & 0 & 0 & + & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & + \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & * & 0 & 0 & * & * & 0 \\ 0 & 0 & 1 & 0 & * & * & 0 \\ 0 & 0 & 0 & 1 & * & * & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Théorème 46

Étant donnée une matrice $A \in M_{n,p}(\mathbb{K})$, il existe une unique matrice échelonnée réduite U obtenue à partir de A par des opérations élémentaires sur les lignes.

Ce théorème permet donc de se ramener par des opérations élémentaires à des matrices dont la structure est beaucoup plus simple : les matrices échelonnées réduites.

Démonstration

Nous admettons l'unicité.
L'existence se démontre grâce à l'algorithme de Gauss. L'idée générale consiste à utiliser des substitutions de lignes pour placer des zéros là où il faut de façon à créer d'abord une forme échelonnée, puis une forme échelonnée réduite.

Soit A une matrice $n \times p$ quelconque.

Partie A. Passage à une forme échelonnée.
Étape A.1. *Choix du pivot.*
On commence par inspecter la première colonne. Soit elle ne contient que des zéros, auquel cas on passe directement à l'étape A.3, soit elle contient au moins un terme non nul. On choisit alors un tel terme, que l'on appelle le ***pivot***. Si c'est le terme a_{11}, on passe directement à l'étape A.2 ; si c'est un terme a_{i1} avec $i \neq 1$, on échange les lignes 1 et i ($L_1 \leftrightarrow L_i$) et on passe à l'étape A.2.
Au terme de l'étape A.1, soit la matrice A a sa première colonne nulle (à gauche) ou bien on obtient une matrice équivalente dont le premier coefficient a'_{11} est non nul (à droite) :

$$\begin{pmatrix} 0 & a_{12} & \cdots & a_{1j} & \cdots & a_{1p} \\ 0 & a_{22} & \cdots & a_{2j} & \cdots & a_{2p} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & a_{i2} & \cdots & a_{ij} & \cdots & a_{ip} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & a_{n2} & \cdots & a_{nj} & \cdots & a_{np} \end{pmatrix} = A \qquad \text{ou bien} \qquad \begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1j} & \cdots & a'_{1p} \\ a'_{21} & a'_{22} & \cdots & a'_{2j} & \cdots & a'_{2p} \\ \vdots & \vdots & & \vdots & & \vdots \\ a'_{i1} & a'_{i2} & \cdots & a'_{ij} & \cdots & a'_{ip} \\ \vdots & \vdots & & \vdots & & \vdots \\ a'_{n1} & a'_{n2} & \cdots & a'_{nj} & \cdots & a'_{np} \end{pmatrix} \sim A.$$

Étape A.2. *Élimination.*
On ne touche plus à la ligne 1, et on se sert du pivot a'_{11} pour éliminer tous les termes a'_{i1} (avec $i \geqslant 2$) situés sous le pivot. Pour cela, il suffit de remplacer la ligne i par elle-même moins $\frac{a'_{i1}}{a'_{11}} \times$ la ligne 1, ceci pour $i = 2, \ldots, n$: $L_2 \leftarrow L_2 - \frac{a'_{21}}{a'_{11}} L_1$, $L_3 \leftarrow L_3 - \frac{a'_{31}}{a'_{11}} L_1, \ldots$
Au terme de l'étape A.2, on a obtenu une matrice de la forme

$$\begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1j} & \cdots & a'_{1p} \\ 0 & a''_{22} & \cdots & a''_{2j} & \cdots & a''_{2p} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & a''_{i2} & \cdots & a''_{ij} & \cdots & a''_{ip} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & a''_{n2} & \cdots & a''_{nj} & \cdots & a''_{np} \end{pmatrix} \sim A.$$

Étape A.3. *Boucle.*

Au début de l'étape A.3, on a obtenu dans tous les cas de figure une matrice de la forme

$$\begin{pmatrix} a_{11}^1 & a_{12}^1 & \cdots & a_{1j}^1 & \cdots & a_{1p}^1 \\ 0 & a_{22}^1 & \cdots & a_{2j}^1 & \cdots & a_{2p}^1 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & a_{i2}^1 & \cdots & a_{ij}^1 & \cdots & a_{ip}^1 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & a_{n2}^1 & \cdots & a_{nj}^1 & \cdots & a_{np}^1 \end{pmatrix} \sim A$$

dont la première colonne est bien celle d'une matrice échelonnée. On va donc conserver cette première colonne. Si $a_{11}^1 \neq 0$, on conserve aussi la première ligne, et l'on repart avec l'étape A.1 en l'appliquant cette fois à la sous-matrice $(n-1)\times(p-1)$ (ci-dessous à gauche : on « oublie » la première ligne et la première colonne de A) ; si $a_{11}^1 = 0$, on repart avec l'étape A.1 en l'appliquant à la sous-matrice $n\times(p-1)$ (à droite, on « oublie » la première colonne) :

$$\begin{pmatrix} a_{22}^1 & \cdots & a_{2j}^1 & \cdots & a_{2p}^1 \\ \vdots & & \vdots & & \vdots \\ a_{i2}^1 & \cdots & a_{ij}^1 & \cdots & a_{ip}^1 \\ \vdots & & \vdots & & \vdots \\ a_{n2}^1 & \cdots & a_{nj}^1 & \cdots & a_{np}^1 \end{pmatrix} \qquad \begin{pmatrix} a_{12}^1 & \cdots & a_{1j}^1 & \cdots & a_{1p}^1 \\ a_{22}^1 & \cdots & a_{2j}^1 & \cdots & a_{2p}^1 \\ \vdots & & \vdots & & \vdots \\ a_{i2}^1 & \cdots & a_{ij}^1 & \cdots & a_{ip}^1 \\ \vdots & & \vdots & & \vdots \\ a_{n2}^1 & \cdots & a_{nj}^1 & \cdots & a_{np}^1 \end{pmatrix}$$

Au terme de cette deuxième itération de la boucle, on aura obtenu une matrice de la forme

$$\begin{pmatrix} a_{11}^1 & a_{12}^1 & \cdots & a_{1j}^1 & \cdots & a_{1p}^1 \\ 0 & a_{22}^2 & \cdots & a_{2j}^2 & \cdots & a_{2p}^2 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{ij}^2 & \cdots & a_{ip}^2 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{nj}^2 & \cdots & a_{np}^2 \end{pmatrix} \sim A,$$

et ainsi de suite.
Comme chaque itération de la boucle travaille sur une matrice qui a une colonne de moins que la précédente, alors au bout d'au plus $p-1$ itérations de la boucle, on aura obtenu une matrice échelonnée.

Partie B. Passage à une forme échelonnée réduite.
Étape B.1. *Homothéties.*
On repère le premier élément non nul de chaque ligne non nulle, et on multiplie cette ligne par l'inverse de cet élément. Exemple : si le premier élément non nul de la ligne i est $\alpha \neq 0$, alors on effectue $L_i \leftarrow \frac{1}{\alpha}L_i$. Ceci crée une matrice échelonnée avec des 1 en position de pivots.

Étape B.2. *Élimination.*
On élimine les termes situés au-dessus des positions de pivot comme précédemment, en procédant à partir du bas à droite de la matrice. Ceci ne modifie pas la structure échelonnée de la matrice en raison de la disposition des zéros dont on part.

Exemple 168

Soit

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 6 \\ -1 & 0 & 1 & 0 \end{pmatrix}.$$

A. Passage à une forme échelonnée.
Première itération de la boucle, étape A.1. Le choix du pivot est tout fait, on garde $a_{11}^1 = 1$.
Première itération de la boucle, étape A.2. On ne fait rien sur la ligne 2 qui contient déjà un zéro en bonne position et on remplace la ligne 3 par $L_3 \leftarrow L_3 + L_1$. On obtient

$$A \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 6 \\ 0 & 2 & 4 & 4 \end{pmatrix}.$$

Deuxième itération de la boucle, étape A.1. Le choix du pivot est tout fait, on garde $a_{22}^2 = 2$.
Deuxième itération de la boucle, étape A.2. On remplace la ligne 3 avec l'opération $L_3 \leftarrow L_3 - L_2$. On obtient

$$A \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & -2 \end{pmatrix}.$$

Cette matrice est échelonnée.

B. Passage à une forme échelonnée réduite.
Étape B.1, homothéties. On multiplie la ligne 2 par $\frac{1}{2}$ et la ligne 3 par $-\frac{1}{2}$ et l'on obtient

$$A \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Étape B.2, première itération. On ne touche plus à la ligne 3 et on remplace la ligne 2 par $L_2 \leftarrow L_2 - 3L_3$ et $L_1 \leftarrow L_1 - 4L_3$. On obtient

$$A \sim \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Étape B.2, deuxième itération. On ne touche plus à la ligne 2 et on remplace la ligne 1 par $L_1 \leftarrow L_1 - 2L_2$. On obtient

$$A \sim \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

qui est bien échelonnée et réduite.

5.5. Matrices élémentaires et inverse d'une matrice

Théorème 47

Soit $A \in M_n(\mathbb{K})$. La matrice A est inversible si et seulement si sa forme échelonnée réduite est la matrice identité I_n.

Démonstration

Notons U la forme échelonnée réduite de A. Et notons E le produit de matrices élémentaires tel que $EA = U$.

$\Longleftarrow$ Si $U = I_n$ alors $EA = I_n$. Ainsi par définition, A est inversible et $A^{-1} = E$.

$\Longrightarrow$ Nous allons montrer que si $U \neq I_n$, alors A n'est pas inversible.

- Supposons $U \neq I_n$. Alors la dernière ligne de U est nulle (sinon il y aurait un pivot sur chaque ligne donc ce serait I_n).
- Cela entraîne que U n'est pas inversible : en effet, pour tout matrice carrée V, la dernière ligne de UV est nulle ; on n'aura donc jamais $UV = I_n$.
- Alors, A n'est pas inversible non plus : en effet, si A était inversible, on aurait $U = EA$ et U serait inversible comme produit de matrices inversibles (E est inversible car c'est un produit de matrices élémentaires qui sont inversibles).

Remarque

Justifions maintenant notre méthode pour calculer A^{-1}.
Nous partons de $(A|I)$ pour arriver par des opérations élémentaires sur les lignes à $(I|B)$. Montrons que $B = A^{-1}$. Faire une opération élémentaire signifie multiplier à gauche par une des matrices élémentaires. Notons E le produit de ces matrices élémentaires. Dire que l'on arrive à la fin du processus à I signifie $EA = I$. Donc $A^{-1} = E$. Comme on fait les mêmes opérations sur la partie droite du tableau, alors on obtient $EI = B$. Donc $B = E$. Conséquence : $B = A^{-1}$.

Corollaire 20

Les assertions suivantes sont équivalentes :

(i) La matrice A est inversible.

(ii) Le système linéaire $AX = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ a une unique solution $X = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$.

(iii) Pour tout second membre B, le système linéaire $AX = B$ a une unique solution X.

Démonstration

Nous avons déjà vu $(i) \Longrightarrow (ii)$ et $(i) \Longrightarrow (iii)$.
Nous allons seulement montrer $(ii) \Longrightarrow (i)$. Nous raisonnons par contraposée : nous allons montrer la proposition équivalente non$(i) \Longrightarrow$ non(ii). Si A n'est pas inversible, alors sa forme échelonnée réduite U contient un premier zéro sur sa diagonale, disons à la place ℓ. Alors U à la forme suivante

$$\begin{pmatrix} 1 & 0 & \cdots & c_1 & * & \cdots & * \\ 0 & \ddots & 0 & \vdots & & \cdots & * \\ 0 & 0 & 1 & c_{\ell-1} & & \cdots & * \\ 0 & \cdots & 0 & 0 & * & \cdots & * \\ 0 & \cdots & 0 & 0 & * & \cdots & * \\ \vdots & \vdots & \vdots & \cdots & 0 & \ddots & \vdots \\ 0 & \cdots & & & \cdots & 0 & * \end{pmatrix}. \quad \text{On note} \quad X = \begin{pmatrix} -c_1 \\ \vdots \\ -c_{\ell-1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

> Alors X n'est pas le vecteur nul, mais UX est le vecteur nul. Comme $A = E^{-1}U$, alors AX est le vecteur nul. Nous avons donc trouvé un vecteur non nul X tel que $AX = 0$.

Mini-exercices

1. Exprimer les systèmes linéaires suivants sous forme matricielle et les résoudre en inversant la matrice : $\begin{cases} 2x+4y=7 \\ -2x+3y=-14 \end{cases}$, $\begin{cases} x+z=1 \\ -2y+3z=1 \\ x+z=1 \end{cases}$, $\begin{cases} x+t=\alpha \\ x-2y=\beta \\ x+y+t=2 \\ y+t=4 \end{cases}$.
2. Écrire les matrices 4×4 correspondant aux opérations élémentaires : $L_2 \leftarrow \frac{1}{3}L_2$, $L_3 \leftarrow L_3 - \frac{1}{4}L_2$, $L_1 \leftrightarrow L_4$. Sans calculs, écrire leurs inverses. Écrire la matrice 4×4 de l'opération $L_1 \leftarrow L_1 - 2L_3 + 3L_4$.
3. Écrire les matrices suivantes sous forme échelonnée, puis échelonnée réduite : $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 0 \\ -2 & -2 & -3 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 2 \\ 1 & -1 & 1 \\ 2 & -2 & 3 \end{pmatrix}$, $\begin{pmatrix} 2 & 0 & -2 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & -2 & 1 & 4 \\ -1 & 2 & -1 & -2 \end{pmatrix}$.

6. Matrices triangulaires, transposition, trace, matrices symétriques

6.1. Matrices triangulaires, matrices diagonales

Soit A une matrice de taille $n \times n$. On dit que A est ***triangulaire inférieure*** si ses éléments au-dessus de la diagonale sont nuls, autrement dit :

$$i < j \implies a_{ij} = 0.$$

Une matrice triangulaire inférieure a la forme suivante :

$$\begin{pmatrix} a_{11} & 0 & \cdots & \cdots & 0 \\ a_{21} & a_{22} & \ddots & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & \ddots & 0 \\ a_{n1} & a_{n2} & \cdots & \cdots & a_{nn} \end{pmatrix}$$

On dit que A est ***triangulaire supérieure*** si ses éléments en-dessous de la diagonale sont nuls, autrement dit :

$$i > j \implies a_{ij} = 0.$$

Une matrice triangulaire supérieure a la forme suivante :

$$\begin{pmatrix} a_{11} & a_{12} & \dots & \dots & \dots & a_{1n} \\ 0 & a_{22} & \dots & \dots & \dots & a_{2n} \\ \vdots & \ddots & \ddots & & & \vdots \\ \vdots & & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & \dots & 0 & a_{nn} \end{pmatrix}$$

Exemple 169

Deux matrices triangulaires inférieures (à gauche), une matrice triangulaire supérieure (à droite) :

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & -1 & 0 \\ 3 & -2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 5 & 0 \\ 1 & -2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & -1 \\ 0 & -1 & -1 \\ 0 & 0 & -1 \end{pmatrix}$$

Une matrice qui est triangulaire inférieure ***et*** triangulaire supérieure est dite ***diagonale***. Autrement dit : $i \neq j \implies a_{ij} = 0$.

Exemple 170

Exemples de matrices diagonales :

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$$

Exemple 171. Puissances d'une matrice diagonale

Si D est une matrice diagonale, il est très facile de calculer ses puissances D^p (par récurrence sur p) :

$$D = \begin{pmatrix} \alpha_1 & 0 & \dots & \dots & 0 \\ 0 & \alpha_2 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \alpha_{n-1} & 0 \\ 0 & \dots & \dots & 0 & \alpha_n \end{pmatrix} \implies D^p = \begin{pmatrix} \alpha_1^p & 0 & \dots & \dots & 0 \\ 0 & \alpha_2^p & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \alpha_{n-1}^p & 0 \\ 0 & \dots & \dots & 0 & \alpha_n^p \end{pmatrix}$$

Théorème 48

Une matrice A de taille $n \times n$, triangulaire, est inversible si et seulement si ses éléments diagonaux sont tous non nuls.

Démonstration

Supposons que A soit triangulaire supérieure.

- Si les éléments de la diagonale sont tous non nuls, alors la matrice A est déjà sous la forme échelonnée. En multipliant chaque ligne i par l'inverse de l'élément diagonal a_{ii}, on obtient des 1 sur la diagonale. De ce fait, la forme échelonnée réduite de A sera la matrice identité. Le théorème 47 permet de conclure que A est inversible.
- Inversement, supposons qu'au moins l'un des éléments diagonaux soit nul et notons $a_{\ell\ell}$ le premier élément nul de la diagonale. En multipliant les lignes 1 à $\ell - 1$ par l'inverse de leur

élément diagonal, on obtient une matrice de la forme

$$\begin{pmatrix} 1 & * & \cdots & & & \cdots & * \\ 0 & \ddots & * & \cdots & & \cdots & * \\ 0 & 0 & 1 & * & & \cdots & * \\ 0 & \cdots & 0 & 0 & * & \cdots & * \\ 0 & \cdots & 0 & 0 & * & \cdots & * \\ \vdots & \vdots & \vdots & \cdots & 0 & \ddots & \vdots \\ 0 & \cdots & & & \cdots & 0 & * \end{pmatrix}.$$

Il est alors clair que la colonne numéro ℓ de la forme échelonnée réduite ne contiendra pas de 1 comme pivot. La forme échelonnée réduite de A ne peut donc pas être I_n et par le théorème 47, A n'est pas inversible.

Dans le cas d'une matrice triangulaire inférieure, on utilise la transposition (qui fait l'objet de la section suivante) et on obtient une matrice triangulaire supérieure. On applique alors la démonstration ci-dessus.

6.2. La transposition

Soit A la matrice de taille $n \times p$

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1p} \\ a_{21} & a_{22} & \dots & a_{2p} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{np} \end{pmatrix}.$$

Définition 89

On appelle ***matrice transposée*** de A la matrice A^T de taille $p \times n$ définie par :

$$A^T = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \vdots & \vdots & & \vdots \\ a_{1p} & a_{2p} & \dots & a_{np} \end{pmatrix}.$$

Autrement dit : le coefficient à la place (i,j) de A^T est a_{ji}. Ou encore la i-ème ligne de A devient la i-ème colonne de A^T (et réciproquement la j-ème colonne de A^T est la j-ème ligne de A).

Notation : La transposée de la matrice A se note aussi souvent ${}^tA$.

Exemple 172

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & -6 \\ -7 & 8 & 9 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 & -7 \\ 2 & 5 & 8 \\ 3 & -6 & 9 \end{pmatrix} \qquad \begin{pmatrix} 0 & 3 \\ 1 & -5 \\ -1 & 2 \end{pmatrix}^T = \begin{pmatrix} 0 & 1 & -1 \\ 3 & -5 & 2 \end{pmatrix} \qquad (1 \quad -2 \quad 5)^T = \begin{pmatrix} 1 \\ -2 \\ 5 \end{pmatrix}$$

L'opération de transposition obéit aux règles suivantes :

Théorème 49

1. $(A+B)^T = A^T + B^T$
2. $(\alpha A)^T = \alpha A^T$
3. $(A^T)^T = A$
4. $\boxed{(AB)^T = B^T A^T}$
5. Si A est inversible, alors A^T l'est aussi et on a $(A^T)^{-1} = (A^{-1})^T$.

Notez bien l'inversion : $(AB)^T = B^T A^T$, comme pour $(AB)^{-1} = B^{-1}A^{-1}$.

6.3. La trace

Dans le cas d'une matrice carrée de taille $n \times n$, les éléments a_{11}, $a_{22}, \dots, a_{nn}$ sont appelés les ***éléments diagonaux***.
Sa ***diagonale principale*** est la diagonale $(a_{11}, a_{22}, \dots, a_{nn})$.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Définition 90

La ***trace*** de la matrice A est le nombre obtenu en additionnant les éléments diagonaux de A. Autrement dit,

$$\boxed{\operatorname{tr} A = a_{11} + a_{22} + \dots + a_{nn}.}$$

Exemple 173

- Si $A = \begin{pmatrix} 2 & 1 \\ 0 & 5 \end{pmatrix}$, alors $\operatorname{tr} A = 2 + 5 = 7$.
- Pour $B = \begin{pmatrix} 1 & 1 & 2 \\ 5 & 2 & 8 \\ 11 & 0 & -10 \end{pmatrix}$, $\operatorname{tr} B = 1 + 2 - 10 = -7$.

Théorème 50

Soient A et B deux matrices $n \times n$. Alors :

1. $\operatorname{tr}(A+B) = \operatorname{tr} A + \operatorname{tr} B$,
2. $\operatorname{tr}(\alpha A) = \alpha \operatorname{tr} A$ pour tout $\alpha \in \mathbb{K}$,
3. $\operatorname{tr}(A^T) = \operatorname{tr} A$,
4. $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

Démonstration

1. Pour tout $1 \leqslant i \leqslant n$, le coefficient (i,i) de $A+B$ est $a_{ii}+b_{ii}$. Ainsi, on a bien $\operatorname{tr}(A+B) = \operatorname{tr}(A) + \operatorname{tr}(B)$.
2. On a $\operatorname{tr}(\alpha A) = \alpha a_{11} + \cdots + \alpha a_{nn} = \alpha(a_{11} + \cdots + a_{nn}) = \alpha \operatorname{tr} A$.
3. Étant donné que la transposition ne change pas les éléments diagonaux, la trace de A est égale à la trace de A^T.
4. Notons c_{ij} les coefficients de AB. Alors par définition

$$c_{ii} = a_{i1}b_{1i} + a_{i2}b_{2i} + \cdots + a_{in}b_{ni}.$$

Ainsi,

$$\begin{array}{rcllll} \operatorname{tr}(AB) & = & a_{11}b_{11} & +a_{12}b_{21} & +\cdots & +a_{1n}b_{n1} \\ & & +a_{21}b_{12} & +a_{22}b_{22} & +\cdots & +a_{2n}b_{n2} \\ & & \vdots & & & \\ & & +a_{n1}b_{1n} & +a_{n2}b_{2n} & +\cdots & +a_{nn}b_{nn}. \end{array}$$

On peut réarranger les termes pour obtenir

$$\begin{array}{rcllll} \operatorname{tr}(AB) & = & a_{11}b_{11} & +a_{21}b_{12} & +\cdots & +a_{n1}b_{1n} \\ & & +a_{12}b_{21} & +a_{22}b_{22} & +\cdots & +a_{n2}b_{2n} \\ & & \vdots & & & \\ & & +a_{1n}b_{n1} & +a_{2n}b_{n2} & +\cdots & +a_{nn}b_{nn}. \end{array}$$

En utilisant la commutativité de la multiplication dans $\mathbb{K}$, la première ligne devient

$$b_{11}a_{11} + b_{12}a_{21} + \cdots + b_{1n}a_{n1}$$

qui vaut le coefficient $(1,1)$ de BA. On note d_{ij} les coefficients de BA. En faisant de même avec les autres lignes, on voit finalement que

$$\operatorname{tr}(AB) = d_{11} + \cdots + d_{nn} = \operatorname{tr}(BA).$$

6.4. Matrices symétriques

Définition 91

Une matrice A de taille $n \times n$ est ***symétrique*** si elle est égale à sa transposée, c'est-à-dire si

$$A = A^T,$$

ou encore si $a_{ij} = a_{ji}$ pour tout $i,j = 1,\ldots,n$. Les coefficients sont donc symétriques par rapport à la diagonale.

Exemple 174

Les matrices suivantes sont symétriques :

$$\begin{pmatrix} 0 & 2 \\ 2 & 4 \end{pmatrix} \qquad \begin{pmatrix} -1 & 0 & 5 \\ 0 & 2 & -1 \\ 5 & -1 & 0 \end{pmatrix}$$

Exemple 175

Pour une matrice B quelconque, les matrices $B \cdot B^T$ et $B^T \cdot B$ sont symétriques.
Preuve : $(BB^T)^T = (B^T)^T B^T = BB^T$. Idem pour $B^T B$.

6.5. Matrices antisymétriques

Définition 92

Une matrice A de taille $n \times n$ est ***antisymétrique*** si

$$A^T = -A,$$

c'est-à-dire si $a_{ij} = -a_{ji}$ pour tout $i, j = 1, \ldots, n$.

Exemple 176

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 4 & 2 \\ -4 & 0 & -5 \\ -2 & 5 & 0 \end{pmatrix}$$

Remarquons que les éléments diagonaux d'une matrice antisymétrique sont toujours tous nuls.

Exemple 177

Toute matrice est la somme d'une matrice symétrique et d'une matrice antisymétrique.

Preuve : Soit A une matrice. Définissons $B = \frac{1}{2}(A + A^T)$ et $C = \frac{1}{2}(A - A^T)$. Alors d'une part $A = B + C$; d'autre part B est symétrique, car $B^T = \frac{1}{2}(A^T + (A^T)^T) = \frac{1}{2}(A^T + A) = B$; et enfin C est antisymétrique, car $C^T = \frac{1}{2}(A^T - (A^T)^T) = -C$.
Exemple :

$$\text{Pour} \quad A = \begin{pmatrix} 2 & 10 \\ 8 & -3 \end{pmatrix} \qquad \text{alors} \qquad A \;=\; \underbrace{\begin{pmatrix} 2 & 9 \\ 9 & -3 \end{pmatrix}}_{\text{symétrique}} \;+\; \underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}_{\text{antisymétrique}}.$$

Mini-exercices

1. Montrer que la somme de deux matrices triangulaires supérieures reste triangulaire supérieure. Montrer que c'est aussi valable pour le produit.
2. Montrer que si A est triangulaire supérieure, alors A^T est triangulaire inférieure. Et si A est diagonale ?
3. Soit $A = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$. Calculer $A^T \cdot A$, puis $A \cdot A^T$.
4. Soit $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Calculer $\operatorname{tr}(A \cdot A^T)$.
5. Soit A une matrice de taille 2×2 inversible. Montrer que si A est symétrique, alors A^{-1} aussi. Et si A est antisymétrique ?
6. Montrer que la décomposition d'une matrice sous la forme « symétrique + antisymé-

trique » est unique.

Auteurs

- D'après un cours de Eva Bayer-Fluckiger, Philippe Chabloz, Lara Thomas de l'École Polytechnique Fédérale de Lausanne,
- et un cours de Sophie Chemla de l'université Pierre et Marie Curie, reprenant des parties de cours de H. Ledret et d'une équipe de l'université de Bordeaux animée par J. Queyrut,
- mixés et révisés par Arnaud Bodin, relu par Vianney Combet.





La notion d'espace vectoriel est une structure fondamentale des mathématiques modernes. Il s'agit de dégager les propriétés communes que partagent des ensembles pourtant très différents. Par exemple, on peut additionner deux vecteurs du plan, et aussi multiplier un vecteur par un réel (pour l'agrandir ou le rétrécir). Mais on peut aussi additionner deux fonctions, ou multiplier une fonction par un réel. Même chose avec les polynômes, les matrices,... Le but est d'obtenir des théorèmes généraux qui s'appliqueront aussi bien aux vecteurs du plan, de l'espace, aux espaces de fonctions, aux polynômes, aux matrices,... La contrepartie de cette grande généralité de situations est que la notion d'espace vectoriel est difficile à appréhender et vous demandera une quantité conséquente de travail ! Il est bon d'avoir d'abord étudié le chapitre « L'espace vectoriel $\mathbb{R}^n$ ».

1. Espace vectoriel (début)

Dans ce chapitre, $\mathbb{K}$ désigne un corps. Dans la plupart des exemples, ce sera le corps des réels $\mathbb{R}$.

1.1. Définition d'un espace vectoriel

Un espace vectoriel est un ensemble formé de vecteurs, de sorte que l'on puisse additionner (et soustraire) deux vecteurs u, v pour en former un troisième $u + v$ (ou $u - v$) et aussi afin que l'on puisse multiplier chaque vecteur u d'un facteur λ pour obtenir un vecteur $\lambda \cdot u$. Voici la définition formelle :

Définition 93

Un ***$\mathbb{K}$-espace vectoriel*** est un ensemble non vide E muni :

- d'une loi de composition interne, c'est-à-dire d'une application de $E \times E$ dans E :

$$\begin{array}{ccc} E \times E & \to & E \\ (u,v) & \mapsto & u+v \end{array}$$

- d'une loi de composition externe, c'est-à-dire d'une application de $\mathbb{K} \times E$ dans E :

$$\begin{array}{ccc} \mathbb{K} \times E & \to & E \\ (\lambda,u) & \mapsto & \lambda \cdot u \end{array}$$

qui vérifient les propriétés suivantes :

1. $u+v=v+u$ (pour tous $u,v \in E$)
2. $u+(v+w)=(u+v)+w$ (pour tous $u,v,w \in E$)
3. Il existe un ***élément neutre*** $0_E \in E$ tel que $u+0_E=u$ (pour tout $u \in E$)
4. Tout $u \in E$ admet un ***symétrique*** u' tel que $u+u'=0_E$. Cet élément u' est noté $-u$.
5. $1 \cdot u = u$ (pour tout $u \in E$)
6. $\lambda \cdot (\mu \cdot u) = (\lambda\mu) \cdot u$ (pour tous $\lambda, \mu \in \mathbb{K}$, $u \in E$)
7. $\lambda \cdot (u+v) = \lambda \cdot u + \lambda \cdot v$ (pour tous $\lambda \in \mathbb{K}$, $u,v \in E$)
8. $(\lambda+\mu) \cdot u = \lambda \cdot u + \mu \cdot u$ (pour tous $\lambda, \mu \in \mathbb{K}$, $u \in E$)

Nous reviendrons en détail sur chacune de ces propriétés juste après des exemples.

1.2. Premiers exemples

Exemple 178. Le $\mathbb{R}$-espace vectoriel $\mathbb{R}^2$

Posons $\mathbb{K}=\mathbb{R}$ et $E=\mathbb{R}^2$. Un élément $u \in E$ est donc un couple (x,y) avec x élément de $\mathbb{R}$ et y élément de $\mathbb{R}$. Ceci s'écrit

$$\mathbb{R}^2 = \{(x,y) \mid x \in \mathbb{R}, y \in \mathbb{R}\}.$$

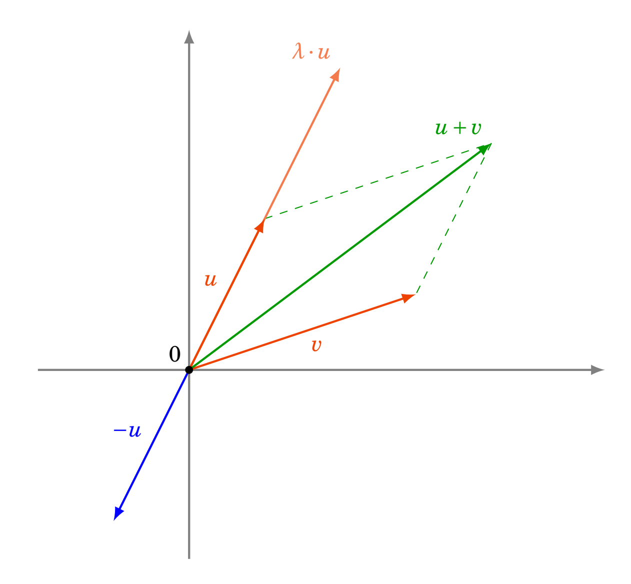
- *Définition de la loi interne.* Si (x,y) et (x',y') sont deux éléments de $\mathbb{R}^2$, alors :

$$(x,y)+(x',y')=(x+x',y+y').$$

- *Définition de la loi externe.* Si λ est un réel et (x,y) est un élément de $\mathbb{R}^2$, alors :

$$\lambda \cdot (x,y) = (\lambda x, \lambda y).$$

L'élément neutre de la loi interne est le vecteur nul $(0,0)$. Le symétrique de (x,y) est $(-x,-y)$, que l'on note aussi $-(x,y)$.



L'exemple suivant généralise le précédent. C'est aussi le bon moment pour lire ou relire le chapitre « L'espace vectoriel $\mathbb{R}^n$ ».

Exemple 179. Le $\mathbb{R}$-espace vectoriel $\mathbb{R}^n$

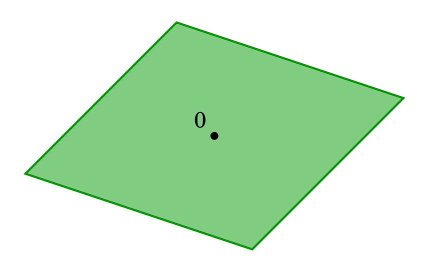
Soit n un entier supérieur ou égal à 1. Posons $\mathbb{K} = \mathbb{R}$ et $E = \mathbb{R}^n$. Un élément $u \in E$ est donc un n-uplet $(x_1, x_2, \ldots, x_n)$ avec $x_1, x_2, \ldots, x_n$ des éléments de $\mathbb{R}$.

- *Définition de la loi interne.* Si $(x_1, \ldots, x_n)$ et $(x'_1, \ldots, x'_n)$ sont deux éléments de $\mathbb{R}^n$, alors :
$$(x_1, \ldots, x_n) + (x'_1, \ldots, x'_n) = (x_1 + x'_1, \ldots, x_n + x'_n).$$
- *Définition de la loi externe.* Si λ est un réel et $(x_1, \ldots, x_n)$ est un élément de $\mathbb{R}^n$, alors :
$$\lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n).$$

L'élément neutre de la loi interne est le vecteur nul $(0, 0, \ldots, 0)$. Le symétrique de $(x_1, \ldots, x_n)$ est $(-x_1, \ldots, -x_n)$, que l'on note $-(x_1, \ldots, x_n)$.
De manière analogue, on peut définir le $\mathbb{C}$-espace vectoriel $\mathbb{C}^n$, et plus généralement le $\mathbb{K}$-espace vectoriel $\mathbb{K}^n$.

Exemple 180

Tout plan passant par l'origine dans $\mathbb{R}^3$ est un espace vectoriel (par rapport aux opérations habituelles sur les vecteurs). Soient $\mathbb{K} = \mathbb{R}$ et $E = \mathscr{P}$ un plan passant par l'origine. Le plan admet une équation de la forme :
$$ax + by + cz = 0$$
où a, b et c sont des réels non tous nuls.



Un élément $u \in E$ est donc un triplet (noté ici comme un vecteur colonne) $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ tel que $ax + by +$

$cz = 0$.

Soient $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ et $\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$ deux éléments de $\mathscr{P}$. Autrement dit,

$$\begin{array}{rrcl} & ax + by + cz & = & 0, \\ \text{et} & ax' + by' + cz' & = & 0. \end{array}$$

Alors $\begin{pmatrix} x+x' \\ y+y' \\ z+z' \end{pmatrix}$ est aussi dans $\mathscr{P}$ car on a bien :

$$a(x + x') + b(y + y') + c(z + z') = 0.$$

Les autres propriétés sont aussi faciles à vérifier : par exemple l'élément neutre est $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$; et si $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ appartient à $\mathscr{P}$, alors $ax + by + cz = 0$, que l'on peut réécrire $a(-x) + b(-y) + c(-z) = 0$ et ainsi $-\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ appartient à $\mathscr{P}$.

Attention ! Un plan ne contenant pas l'origine n'est pas un espace vectoriel, car justement il ne contient pas le vecteur nul $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$.

1.3. Terminologie et notations

Rassemblons les définitions déjà vues.

- On appelle les éléments de E des ***vecteurs***. Au lieu de $\mathbb{K}$-espace vectoriel, on dit aussi espace vectoriel sur $\mathbb{K}$.
- Les éléments de $\mathbb{K}$ seront appelés des ***scalaires***.
- L'***élément neutre*** 0_E s'appelle aussi le ***vecteur nul***. Il ne doit pas être confondu avec l'élément 0 de $\mathbb{K}$. Lorsqu'il n'y aura pas de risque de confusion, 0_E sera aussi noté 0.
- Le ***symétrique*** $-u$ d'un vecteur $u \in E$ s'appelle aussi l'***opposé***.
- La loi de composition interne sur E (notée usuellement $+$) est appelée couramment l'addition et $u + u'$ est appelée somme des vecteurs u et u'.
- La loi de composition externe sur E est appelée couramment multiplication par un scalaire. La multiplication du vecteur u par le scalaire λ sera souvent notée simplement λu, au lieu de $\lambda \cdot u$.

Somme de n vecteurs. Il est possible de définir, par récurrence, l'addition de n vecteurs, $n \geqslant 2$. La structure d'espace vectoriel permet de définir l'addition de deux vecteurs (et initialise le processus). Si maintenant la somme de $n-1$ vecteurs est définie, alors la somme de n vecteurs $v_1, v_2, \ldots, v_n$ est définie par

$$v_1 + v_2 + \cdots + v_n = (v_1 + v_2 + \cdots + v_{n-1}) + v_n.$$

L'associativité de la loi $+$ nous permet de ne pas mettre de parenthèses dans la somme $v_1 + v_2 + \cdots + v_n$.

On notera $v_1 + v_2 + \cdots + v_n = \sum_{i=1}^{n} v_i$.

1.4. Mini-exercices

1. Vérifier les 8 axiomes qui font de $\mathbb{R}^3$ un $\mathbb{R}$-espace vectoriel.
2. Idem pour une droite $\mathscr{D}$ de $\mathbb{R}^3$ passant par l'origine définie par $\begin{cases} ax + by + cz & = & 0 \\ a'x + b'y + c'z & = & 0 \end{cases}$.
3. Justifier que les ensembles suivants *ne sont pas* des espaces vectoriels : $\{(x, y) \in \mathbb{R}^2 \mid xy = 0\}$; $\{(x, y) \in \mathbb{R}^2 \mid x = 1\}$; $\{(x, y) \in \mathbb{R}^2 \mid x \geqslant 0 \text{ et } y \geqslant 0\}$; $\{(x, y) \in \mathbb{R}^2 \mid -1 \leqslant x \leqslant 1 \text{ et } -1 \leqslant y \leqslant 1\}$.

4. Montrer par récurrence que si les v_i sont des éléments d'un $\mathbb{K}$-espace vectoriel E, alors pour tous $\lambda_i \in \mathbb{K}$: $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n \in E$.

2. Espace vectoriel (fin)

2.1. Détail des axiomes de la définition

Revenons en détail sur la définition d'un espace vectoriel. Soit donc E un $\mathbb{K}$-espace vectoriel. Les éléments de E seront appelés des ***vecteurs***. Les éléments de $\mathbb{K}$ seront appelés des ***scalaires***.

Loi interne.

La loi de composition interne dans E, c'est une application de $E \times E$ dans E :

$$\begin{array}{ccc} E \times E & \to & E \\ (u,v) & \mapsto & u+v \end{array}$$

C'est-à-dire qu'à partir de deux vecteurs u et v de E, on nous en fournit un troisième, qui sera noté $u+v$.

La loi de composition interne dans E et la somme dans $\mathbb{K}$ seront toutes les deux notées +, mais le contexte permettra de déterminer aisément de quelle loi il s'agit.

Loi externe.

La loi de composition externe, c'est une application de $\mathbb{K} \times E$ dans E :

$$\begin{array}{ccc} \mathbb{K} \times E & \to & E \\ (\lambda,u) & \mapsto & \lambda \cdot u \end{array}$$

C'est-à-dire qu'à partir d'un scalaire $\lambda \in \mathbb{K}$ et d'un vecteur $u \in E$, on nous fournit un autre vecteur, qui sera noté $\lambda \cdot u$.

Axiomes relatifs à la loi interne.

1. ***Commutativité.*** Pour tous $u,v \in E$, $u+v = v+u$. On peut donc additionner des vecteurs dans l'ordre que l'on souhaite.
2. ***Associativité.*** Pour tous $u,v,w \in E$, on a $u+(v+w) = (u+v)+w$. Conséquence : on peut « oublier » les parenthèses et noter sans ambiguïté $u+v+w$.
3. Il existe un ***élément neutre***, c'est-à-dire qu'il existe un élément de E, noté 0_E, vérifiant : pour tout $u \in E$, $u + 0_E = u$ (et on a aussi $0_E + u = u$ par commutativité). Cet élément 0_E s'appelle aussi le ***vecteur nul***.
4. Tout élément u de E admet un ***symétrique*** (ou ***opposé***), c'est-à-dire qu'il existe un élément u' de E tel que $u+u' = 0_E$ (et on a aussi $u'+u = 0_E$ par commutativité). Cet élément u' de E est noté $-u$.

Proposition 108

- S'il existe un élément neutre 0_E vérifiant l'axiome (3) ci-dessus, alors il est unique.
- Soit u un élément de E. S'il existe un élément symétrique u' de E vérifiant l'axiome (4), alors il est unique.

Démonstration

- Soient 0_E et $0'_E$ deux éléments vérifiant la définition de l'élément neutre. On a alors, pour tout élément u de E :
$$u + 0_E = 0_E + u = u \qquad \text{et} \qquad u + 0'_E = 0'_E + u = u$$
  - Alors, la première propriété utilisée avec $u = 0'_E$ donne $0'_E + 0_E = 0_E + 0'_E = 0'_E$.
  - La deuxième propriété utilisée avec $u = 0_E$ donne $0_E + 0'_E = 0'_E + 0_E = 0_E$.
  - En comparant ces deux résultats, il vient $0_E = 0'_E$.
- Supposons qu'il existe deux symétriques de u notés u' et u''. On a :
$$u + u' = u' + u = 0_E \qquad \text{et} \qquad u + u'' = u'' + u = 0_E.$$
  Calculons $u' + (u + u'')$ de deux façons différentes, en utilisant l'associativité de la loi + et les relations précédentes.
  - $u' + (u + u'') = u' + 0_E = u'$
  - $u' + (u + u'') = (u' + u) + u'' = 0_E + u'' = u''$
  - On en déduit $u' = u''$.

Remarque

Les étudiants connaissant la théorie des groupes reconnaîtront, dans les quatre premiers axiomes ci-dessus, les axiomes caractérisant un groupe commutatif.

Axiomes relatifs à la loi externe.

5. Soit 1 l'élément neutre de la multiplication de $\mathbb{K}$. Pour tout élément u de E, on a
$$1 \cdot u = u.$$
6. Pour tous éléments λ et μ de $\mathbb{K}$ et pour tout élément u de E, on a
$$\lambda \cdot (\mu \cdot u) = (\lambda \times \mu) \cdot u.$$

Axiomes liant les deux lois.

7. ***Distributivité*** par rapport à l'addition des vecteurs. Pour tout élément λ de $\mathbb{K}$ et pour tous éléments u et v de E, on a
$$\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v.$$
8. ***Distributivité*** par rapport à l'addition des scalaires. Pour tous λ et μ de $\mathbb{K}$ et pour tout élément u de E, on a :
$$(\lambda + \mu) \cdot u = \lambda \cdot u + \mu \cdot u.$$

La loi interne et la loi externe doivent donc satisfaire ces huit axiomes pour que $(E, +, \cdot)$ soit un espace vectoriel sur $\mathbb{K}$.

2.2. Exemples

Dans tous les exemples qui suivent, la vérification des axiomes se fait simplement et est laissée au soin des étudiants. Seules seront indiquées, dans chaque cas, les valeurs de l'élément neutre de la loi interne et du symétrique d'un élément.

Exemple 181. L'espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$

L'ensemble des fonctions $f : \mathbb{R} \longrightarrow \mathbb{R}$ est noté $\mathscr{F}(\mathbb{R},\mathbb{R})$. Nous le munissons d'une structure de $\mathbb{R}$-espace vectoriel de la manière suivante.

- *Loi interne.* Soient f et g deux éléments de $\mathscr{F}(\mathbb{R},\mathbb{R})$. La fonction $f+g$ est définie par :

$$\forall x \in \mathbb{R} \quad (f+g)(x) = f(x)+g(x)$$

(où le signe + désigne la loi interne de $\mathscr{F}(\mathbb{R},\mathbb{R})$ dans le membre de gauche et l'addition dans $\mathbb{R}$ dans le membre de droite).

- *Loi externe.* Si λ est un nombre réel et f une fonction de $\mathscr{F}(\mathbb{R},\mathbb{R})$, la fonction $\lambda \cdot f$ est définie par l'image de tout réel x comme suit :

$$\forall x \in \mathbb{R} \quad (\lambda \cdot f)(x) = \lambda \times f(x).$$

(Nous désignons par $\cdot$ la loi externe de $\mathscr{F}(\mathbb{R},\mathbb{R})$ et par $\times$ la multiplication dans $\mathbb{R}$. Avec l'habitude on oubliera les signes de multiplication : $(\lambda f)(x) = \lambda f(x)$.)

- *Élément neutre.* L'élément neutre pour l'addition est la fonction nulle, définie par :

$$\forall x \in \mathbb{R} \quad f(x) = 0.$$

On peut noter cette fonction $0_{\mathscr{F}(\mathbb{R},\mathbb{R})}$.

- *Symétrique.* Le symétrique de l'élément f de $\mathscr{F}(\mathbb{R},\mathbb{R})$ est l'application g de $\mathbb{R}$ dans $\mathbb{R}$ définie par :

$$\forall x \in \mathbb{R} \quad g(x) = -f(x).$$

Le symétrique de f est noté $-f$.

Exemple 182. Le $\mathbb{R}$-espace vectoriel des suites réelles

On note $\mathscr{S}$ l'ensemble des suites réelles $(u_n)_{n\in\mathbb{N}}$. Cet ensemble peut être vu comme l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{R}$; autrement dit $\mathscr{S} = \mathscr{F}(\mathbb{N},\mathbb{R})$.

- *Loi interne.* Soient $u = (u_n)_{n\in\mathbb{N}}$ et $v = (v_n)_{n\in\mathbb{N}}$ deux suites appartenant à $\mathscr{S}$. La suite $u+v$ est la suite $w = (w_n)_{n\in\mathbb{N}}$ dont le terme général est défini par

$$\forall n \in \mathbb{N} \quad w_n = u_n + v_n$$

(où $u_n + v_n$ désigne la somme de u_n et de v_n dans $\mathbb{R}$).

- *Loi externe.* Si λ est un nombre réel et $u = (u_n)_{n\in\mathbb{N}}$ un élément de $\mathscr{S}$, $\lambda \cdot u$ est la suite $v = (v_n)_{n\in\mathbb{N}}$ définie par

$$\forall n \in \mathbb{N} \quad v_n = \lambda \times u_n$$

où $\times$ désigne la multiplication dans $\mathbb{R}$.

- *Élément neutre.* L'élément neutre de la loi interne est la suite dont tous les termes sont nuls.
- *Symétrique.* Le symétrique de la suite $u = (u_n)_{n\in\mathbb{N}}$ est la suite $u' = (u'_n)_{n\in\mathbb{N}}$ définie par :

$$\forall n \in \mathbb{N} \quad u'_n = -u_n.$$

Elle est notée $-u$.

Exemple 183. Les matrices

L'ensemble $M_{n,p}(\mathbb{R})$ des matrices à n lignes et p colonnes à coefficients dans $\mathbb{R}$ est muni d'une structure de $\mathbb{R}$-espace vectoriel. La loi interne est l'addition de deux matrices. La loi externe est la multiplication d'une matrice par un scalaire. L'élément neutre pour la loi interne est la matrice nulle (tous les coefficients sont nuls). Le symétrique de la matrice $A = (a_{i,j})$ est la matrice $(-a_{i,j})$. De même, l'ensemble $M_{n,p}(\mathbb{K})$ des matrices à coefficients dans $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel.

Autres exemples :

1. L'espace vectoriel $\mathbb{R}[X]$ des polynômes $P(X) = a_nX^n + \cdots + a_2X^2 + a_1X + a_0$. L'addition est l'addition de deux polynômes $P(X)+Q(X)$, la multiplication par un scalaire $\lambda \in \mathbb{R}$ est $\lambda \cdot P(X)$. L'élément neutre est le polynôme nul. L'opposé de $P(X)$ est $-P(X)$.
2. L'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$; l'ensemble des fonctions dérivables de $\mathbb{R}$ dans $\mathbb{R}$,...
3. $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel : addition $z + z'$ de deux nombres complexes, multiplication λz par un scalaire $\lambda \in \mathbb{R}$. L'élément neutre est le nombre complexe 0 et le symétrique du nombre complexe z est $-z$.

2.3. Règles de calcul

Proposition 109

Soit E un espace vectoriel sur un corps $\mathbb{K}$. Soient $u \in E$ et $\lambda \in \mathbb{K}$. Alors on a :

1. $0 \cdot u = 0_E$
2. $\lambda \cdot 0_E = 0_E$
3. $(-1) \cdot u = -u$
4. $\boxed{\lambda \cdot u = 0_E \iff \lambda = 0 \ \text{ ou } \ u = 0_E}$

L'opération qui à (u,v) associe $u+(-v)$ s'appelle la ***soustraction***. Le vecteur $u+(-v)$ est noté $u-v$. Les propriétés suivantes sont satisfaites : $\lambda(u-v) = \lambda u - \lambda v$ et $(\lambda - \mu)u = \lambda u - \mu u$.

Démonstration

Les démonstrations des propriétés sont des manipulations sur les axiomes définissant les espaces vectoriels.

1. – Le point de départ de la démonstration est l'égalité dans $\mathbb{K}$: $0+0=0$.
   – D'où, pour tout vecteur de E, l'égalité $(0+0)\cdot u = 0 \cdot u$.
   – Donc, en utilisant la distributivité de la loi externe par rapport à la loi interne et la définition de l'élément neutre, on obtient $0 \cdot u + 0 \cdot u = 0 \cdot u$. On peut rajouter l'élément neutre dans le terme de droite, pour obtenir : $0 \cdot u + 0 \cdot u = 0 \cdot u + 0_E$.
   – En ajoutant $-(0 \cdot u)$ de chaque côté de l'égalité, on obtient : $0 \cdot u = 0_E$.
2. La preuve est semblable en partant de l'égalité $0_E + 0_E = 0_E$.
3. Montrer $(-1)\cdot u = -u$ signifie exactement que $(-1)\cdot u$ est le symétrique de u, c'est-à-dire vérifie $u + (-1)\cdot u = 0_E$. En effet :

$$u + (-1)\cdot u = 1 \cdot u + (-1)\cdot u = (1 + (-1))\cdot u = 0 \cdot u = 0_E.$$

4. On sait déjà que si $\lambda = 0$ ou $u = 0_E$, alors les propriétés précédentes impliquent $\lambda \cdot u = 0_E$.

Pour la réciproque, soient $\lambda \in \mathbb{K}$ un scalaire et $u \in E$ un vecteur tels que $\lambda \cdot u = 0_E$.
Supposons λ différent de 0. On doit alors montrer que $u = 0_E$.

- Comme $\lambda \neq 0$, alors λ est inversible pour le produit dans le corps $\mathbb{K}$. Soit λ^{-1} son inverse.
- En multipliant par λ^{-1} les deux membres de l'égalité $\lambda \cdot u = 0_E$, il vient : $\lambda^{-1} \cdot (\lambda \cdot u) = \lambda^{-1} \cdot 0_E$.
- D'où en utilisant les propriétés de la multiplication par un scalaire $(\lambda^{-1} \times \lambda) \cdot u = 0_E$ et donc $1 \cdot u = 0_E$.
- D'où $u = 0_E$.

2.4. Mini-exercices

1. Justifier si les objets suivants sont des espaces vectoriels.
   (a) L'ensemble des fonctions réelles sur $[0,1]$, continues, positives ou nulles, pour l'addition et le produit par un réel.
   (b) L'ensemble des fonctions réelles sur $\mathbb{R}$ vérifiant $\lim_{x\to+\infty} f(x) = 0$ pour les mêmes opérations.
   (c) L'ensemble des fonctions sur $\mathbb{R}$ telles que $f(3) = 7$.
   (d) L'ensemble $\mathbb{R}_+^*$ pour les opérations $x \oplus y = xy$ et $\lambda \cdot x = x^\lambda$ ($\lambda \in \mathbb{R}$).
   (e) L'ensemble des points (x, y) de $\mathbb{R}^2$ vérifiant $\sin(x + y) = 0$.
   (f) L'ensemble des vecteurs (x, y, z) de $\mathbb{R}^3$ orthogonaux au vecteur $(-1, 3, -2)$.
   (g) L'ensemble des fonctions de classe $\mathscr{C}^2$ vérifiant $f'' + f = 0$.
   (h) L'ensemble des fonctions continues sur $[0,1]$ vérifiant $\int_0^1 f(x) \sin x \, dx = 0$.
   (i) L'ensemble des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{R})$ vérifiant $a + d = 0$.
2. Prouver les propriétés de la soustraction : $\lambda \cdot (u - v) = \lambda \cdot u - \lambda \cdot v$ et $(\lambda - \mu) \cdot u = \lambda \cdot u - \mu \cdot u$.

3. Sous-espace vectoriel (début)

Il est vite fatiguant de vérifier les 8 axiomes qui font d'un ensemble un espace vectoriel. Heureusement, il existe une manière rapide et efficace de prouver qu'un ensemble est un espace vectoriel : grâce à la notion de sous-espace vectoriel.

3.1. Définition d'un sous-espace vectoriel

Définition 94

Soit E un $\mathbb{K}$-espace vectoriel. Une partie F de E est appelée un ***sous-espace vectoriel*** si :

- $0_E \in F$,
- $u + v \in F$ pour tous $u, v \in F$,
- $\lambda \cdot u \in F$ pour tout $\lambda \in \mathbb{K}$ et tout $u \in F$.

Remarque

Expliquons chaque condition.

- La première condition signifie que le vecteur nul de E doit aussi être dans F. En fait il suffit même de prouver que F est non vide.
- La deuxième condition, c'est dire que F est stable pour l'addition : la somme $u + v$ de deux vecteurs u, v de F est bien sûr un vecteur de E (car E est un espace vectoriel), mais ici on exige que $u + v$ soit un élément de F.

– La troisième condition, c'est dire que F est stable pour la multiplication par un scalaire.

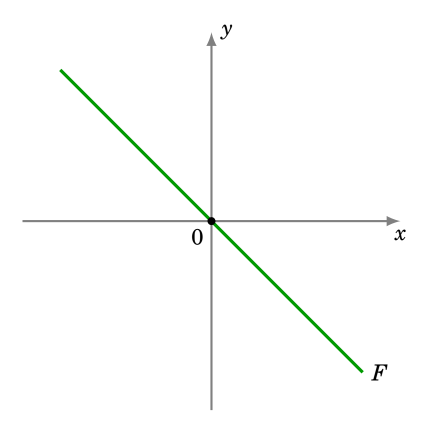
Exemple 184. Exemples immédiats

1. L'ensemble $F = \{(x,y) \in \mathbb{R}^2 \mid x+y=0\}$ est un sous-espace vectoriel de $\mathbb{R}^2$. En effet :

   (a) $(0,0) \in F$,

   (b) si $u = (x_1, y_1)$ et $v = (x_2, y_2)$ appartiennent à F, alors $x_1 + y_1 = 0$ et $x_2 + y_2 = 0$ donc $(x_1+x_2)+(y_1+y_2) = 0$ et ainsi $u+v = (x_1+x_2, y_1+y_2)$ appartient à F,

   (c) si $u = (x,y) \in F$ et $\lambda \in \mathbb{R}$, alors $x+y=0$ donc $\lambda x + \lambda y = 0$, d'où $\lambda u \in F$.

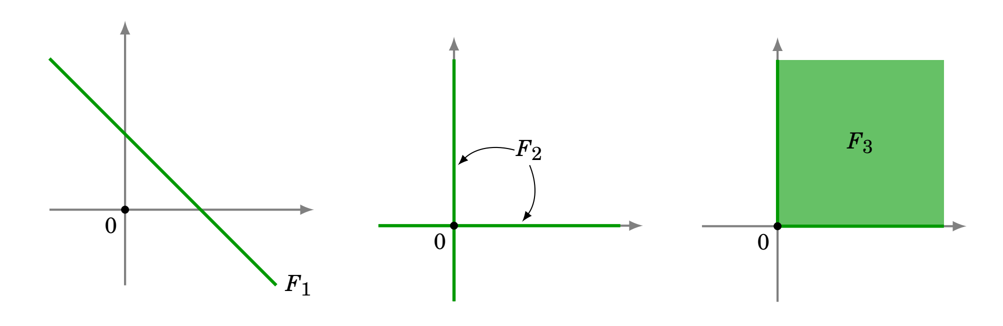


2. L'ensemble des fonctions continues sur $\mathbb{R}$ est un sous-espace vectoriel de l'espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Preuve : la fonction nulle est continue ; la somme de deux fonctions continues est continue ; une constante fois une fonction continue est une fonction continue.
3. L'ensemble des suites réelles convergentes est un sous-espace vectoriel de l'espace vectoriel des suites réelles.

Voici des sous-ensembles qui *ne sont pas* des sous-espaces vectoriels.

Exemple 185

1. L'ensemble $F_1 = \{(x,y) \in \mathbb{R}^2 \mid x+y=2\}$ n'est pas un sous-espace vectoriel de $\mathbb{R}^2$. En effet le vecteur nul $(0,0)$ n'appartient pas à F_1.
2. L'ensemble $F_2 = \{(x,y) \in \mathbb{R}^2 \mid x = 0 \text{ ou } y = 0\}$ n'est pas un sous-espace vectoriel de $\mathbb{R}^2$. En effet les vecteurs $u = (1,0)$ et $v = (0,1)$ appartiennent à F_2, mais pas le vecteur $u+v = (1,1)$.
3. L'ensemble $F_3 = \{(x,y) \in \mathbb{R}^2 \mid x \geqslant 0 \text{ et } y \geqslant 0\}$ n'est pas un sous-espace vectoriel de $\mathbb{R}^2$. En effet le vecteur $u = (1,1)$ appartient à F_3 mais, pour $\lambda = -1$, le vecteur $-u = (-1,-1)$ n'appartient pas à F_3.



3.2. Un sous-espace vectoriel est un espace vectoriel

La notion de sous-espace vectoriel prend tout son intérêt avec le théorème suivant : un sous-espace vectoriel est lui-même un espace vectoriel. C'est ce théorème qui va nous fournir plein d'exemples d'espaces vectoriels.

Théorème 51

Soient E un $\mathbb{K}$-espace vectoriel et F un sous-espace vectoriel de E. Alors F est lui-même un $\mathbb{K}$-espace vectoriel pour les lois induites par E.

Méthodologie. Pour répondre à une question du type « L'ensemble F est-il un espace vectoriel ? », une façon efficace de procéder est de trouver un espace vectoriel E qui contient F, puis prouver que F est un sous-espace vectoriel de E. Il y a seulement trois propriétés à vérifier au lieu de huit !

Exemple 186

1. Est-ce que l'ensemble des fonctions paires (puis des fonctions impaires) forme un espace vectoriel (sur $\mathbb{R}$ avec les lois usuelles sur les fonctions) ?
   Notons $\mathscr{P}$ l'ensemble des fonctions paires et $\mathscr{I}$ l'ensemble des fonctions impaires. Ce sont deux sous-ensembles de l'espace vectoriel $\mathscr{F}(\mathbb{R},\mathbb{R})$ des fonctions.
$$\mathscr{P} = \left\{f \in \mathscr{F}(\mathbb{R},\mathbb{R}) \mid \forall x \in \mathbb{R}, f(-x) = f(x)\right\}$$
$$\mathscr{I} = \left\{f \in \mathscr{F}(\mathbb{R},\mathbb{R}) \mid \forall x \in \mathbb{R}, f(-x) = -f(x)\right\}$$
   $\mathscr{P}$ et $\mathscr{I}$ sont des sous-espaces vectoriels de $\mathscr{F}(\mathbb{R},\mathbb{R})$. C'est très simple à vérifier, par exemple pour $\mathscr{P}$:
   (a) la fonction nulle est une fonction paire,
   (b) si $f,g \in \mathscr{P}$ alors $f+g \in \mathscr{P}$,
   (c) si $f \in \mathscr{P}$ et si $\lambda \in \mathbb{R}$ alors $\lambda f \in \mathscr{P}$.
   Par le théorème 51, $\mathscr{P}$ est un espace vectoriel (de même pour $\mathscr{I}$).
2. Est-ce que l'ensemble $\mathscr{S}_n$ des matrices symétriques de taille n est un espace vectoriel (sur $\mathbb{R}$ avec les lois usuelles sur les matrices) ?
   $\mathscr{S}_n$ est un sous-ensemble de l'espace vectoriel $M_n(\mathbb{R})$. Et c'est même un sous-espace vectoriel. Il suffit en effet de vérifier que la matrice nulle est symétrique, que la somme de deux matrices symétriques est encore symétrique et finalement que le produit d'une matrice symétrique par un scalaire est une matrice symétrique. Par le théorème 51, $\mathscr{S}_n$ est un espace vectoriel.

Démonstration . Preuve du théorème 51

Soit F un sous-espace vectoriel d'un espace vectoriel $(E,+,\cdot)$. La stabilité de F pour les deux lois permet de munir cet ensemble d'une loi de composition interne et d'une loi de composition externe, en restreignant à F les opérations définies dans E. Les propriétés de commutativité et d'associativité de l'addition, ainsi que les quatre axiomes relatifs à la loi externe sont vérifiés, car ils sont satisfaits dans E donc en particulier dans F, qui est inclus dans E.
L'existence d'un élément neutre découle de la définition de sous-espace vectoriel. Il reste seulement à justifier que si $u \in F$, alors son symétrique $-u$ appartient à F.
Fixons $u \in F$. Comme on a aussi $u \in E$ et que E est un espace vectoriel alors il existe un élément de

E, noté $-u$, tel que $u+(-u)=0_E$. Comme u est élément de F, alors pour $\lambda=-1$, $(-1)u \in F$. Et ainsi $-u$ appartient à F.

Un autre exemple d'espace vectoriel est donné par l'ensemble des solutions d'un système linéaire homogène. Soit $AX=0$ un système de n équations à p inconnues :

$$\begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

On a alors

Théorème 52

Soit $A \in M_{n,p}(\mathbb{R})$. Soit $AX=0$ un système d'équations linéaires homogènes à p variables. Alors l'ensemble des vecteurs solutions est un sous-espace vectoriel de $\mathbb{R}^p$.

Démonstration

Soit F l'ensemble des vecteurs $X \in \mathbb{R}^p$ solutions de l'équation $AX=0$. Vérifions que F est un sous-espace vectoriel de $\mathbb{R}^p$.

- Le vecteur 0 est un élément de F.
- F est stable par addition : si X et X' sont des vecteurs solutions, alors $AX=0$ et $AX'=0$, donc $A(X+X')=AX+AX'=0$, et ainsi $X+X' \in F$.
- F est stable par multiplication par un scalaire : si X est un vecteur solution, on a aussi $A(\lambda X)=\lambda(AX)=\lambda 0=0$, ceci pour tout $\lambda \in \mathbb{R}$. Donc $\lambda X \in F$.

Exemple 187

Considérons le système

$$\begin{pmatrix} 1 & -2 & 3 \\ 2 & -4 & 6 \\ 3 & -6 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

L'ensemble des solutions $F \subset \mathbb{R}^3$ de ce système est :

$$F = \{(x=2s-3t, y=s, z=t) \mid s,t \in \mathbb{R}\}.$$

Par le théorème 52, F est un sous-espace vectoriel de $\mathbb{R}^3$. Donc par le théorème 51, F est un espace vectoriel.

Une autre façon de voir les choses est d'écrire que les éléments de F sont ceux qui vérifient l'équation $(x=2y-3z)$. Autrement dit, F est d'équation $(x-2y+3z=0)$. L'ensemble des solutions F est donc un plan passant par l'origine. Nous avons déjà vu que ceci est un espace vectoriel.

3.3. Mini-exercices

Parmi les ensembles suivants, reconnaître ceux qui sont des sous-espaces vectoriels :

1. $\{(x,y,z) \in \mathbb{R}^3 \mid x+y=0\}$
2. $\{(x,y,z,t) \in \mathbb{R}^4 \mid x=t \text{ et } y=z\}$
3. $\{(x,y,z) \in \mathbb{R}^3 \mid z=1\}$

4. $\{(x,y)\in\mathbb{R}^2 \mid x^2+xy\geqslant 0\}$
5. $\{(x,y)\in\mathbb{R}^2 \mid x^2+y^2\geqslant 1\}$
6. $\{f\in\mathscr{F}(\mathbb{R},\mathbb{R}) \mid f(0)=1\}$
7. $\{f\in\mathscr{F}(\mathbb{R},\mathbb{R}) \mid f(1)=0\}$
8. $\{f\in\mathscr{F}(\mathbb{R},\mathbb{R}) \mid f \text{ est croissante }\}$
9. $\{(u_n)_{n\in\mathbb{N}} \mid (u_n) \text{ tend vers } 0\}$

4. Sous-espace vectoriel (milieu)

4.1. Combinaisons linéaires

Définition 95

Soit $n\geqslant 1$ un entier, soient $v_1,v_2,\dots,v_n$, n vecteurs d'un espace vectoriel E. Tout vecteur de la forme

$$u=\lambda_1v_1+\lambda_2v_2+\dots+\lambda_nv_n$$

(où $\lambda_1,\lambda_2,\dots,\lambda_n$ sont des éléments de $\mathbb{K}$) est appelé ***combinaison linéaire*** des vecteurs $v_1,v_2,\dots,v_n$. Les scalaires $\lambda_1,\lambda_2,\dots,\lambda_n$ sont appelés ***coefficients*** de la combinaison linéaire.

Remarque : Si $n=1$, alors $u=\lambda_1v_1$ et on dit que u est ***colinéaire*** à v_1.

Exemple 188

1. Dans le $\mathbb{R}$-espace vectoriel $\mathbb{R}^3$, $(3,3,1)$ est combinaison linéaire des vecteurs $(1,1,0)$ et $(1,1,1)$ car on a l'égalité
$$(3,3,1)=2(1,1,0)+(1,1,1).$$
2. Dans le $\mathbb{R}$-espace vectoriel $\mathbb{R}^2$, le vecteur $u=(2,1)$ *n'est pas* colinéaire au vecteur $v_1=(1,1)$ car s'il l'était, il existerait un réel λ tel que $u=\lambda v_1$, ce qui équivaudrait à l'égalité $(2,1)=(\lambda,\lambda)$.
3. Soit $E=\mathscr{F}(\mathbb{R},\mathbb{R})$ l'espace vectoriel des fonctions réelles. Soient f_0, f_1, f_2 et f_3 les fonctions définies par :
$$\forall x\in\mathbb{R}\quad f_0(x)=1,\ f_1(x)=x,\ f_2(x)=x^2,\ f_3(x)=x^3.$$
Alors la fonction f définie par
$$\forall x\in\mathbb{R}\quad f(x)=x^3-2x^2-7x-4$$
est combinaison linéaire des fonctions f_0,f_1,f_2,f_3 puisque l'on a l'égalité
$$f=f_3-2f_2-7f_1-4f_0.$$
4. Dans $M_{2,3}(\mathbb{R})$, on considère $A=\begin{pmatrix}1&1&3\\0&-1&4\end{pmatrix}$. On peut écrire A naturellement sous la forme suivante d'une combinaison linéaire de matrices élémentaires (des zéros partout, sauf un 1) :
$$A=\begin{pmatrix}1&0&0\\0&0&0\end{pmatrix}+\begin{pmatrix}0&1&0\\0&0&0\end{pmatrix}+3\begin{pmatrix}0&0&1\\0&0&0\end{pmatrix}-\begin{pmatrix}0&0&0\\0&1&0\end{pmatrix}+4\begin{pmatrix}0&0&0\\0&0&1\end{pmatrix}.$$

Voici deux exemples plus compliqués.

Exemple 189

Soient $u = \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}$ et $v = \begin{pmatrix} 6 \\ 4 \\ 2 \end{pmatrix}$ deux vecteurs de $\mathbb{R}^3$. Montrons que $w = \begin{pmatrix} 9 \\ 2 \\ 7 \end{pmatrix}$ est combinaison linéaire de u et v. On cherche donc λ et μ tels que $w = \lambda u + \mu v$:

$$\begin{pmatrix} 9 \\ 2 \\ 7 \end{pmatrix} = \lambda \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix} + \mu \begin{pmatrix} 6 \\ 4 \\ 2 \end{pmatrix} = \begin{pmatrix} \lambda \\ 2\lambda \\ -\lambda \end{pmatrix} + \begin{pmatrix} 6\mu \\ 4\mu \\ 2\mu \end{pmatrix} = \begin{pmatrix} \lambda + 6\mu \\ 2\lambda + 4\mu \\ -\lambda + 2\mu \end{pmatrix}.$$

On a donc

$$\begin{cases} 9 &= \lambda + 6\mu \\ 2 &= 2\lambda + 4\mu \\ 7 &= -\lambda + 2\mu. \end{cases}$$

Une solution de ce système est $(\lambda = -3, \mu = 2)$, ce qui implique que w est combinaison linéaire de u et v. On vérifie que l'on a bien

$$\begin{pmatrix} 9 \\ 2 \\ 7 \end{pmatrix} = -3 \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix} + 2 \begin{pmatrix} 6 \\ 4 \\ 2 \end{pmatrix}.$$

Exemple 190

Soient $u = \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}$ et $v = \begin{pmatrix} 6 \\ 4 \\ 2 \end{pmatrix}$. Montrons que $w = \begin{pmatrix} 4 \\ -1 \\ 8 \end{pmatrix}$ n'est pas une combinaison linéaire de u et v. L'égalité

$$\begin{pmatrix} 4 \\ -1 \\ 8 \end{pmatrix} = \lambda \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix} + \mu \begin{pmatrix} 6 \\ 4 \\ 2 \end{pmatrix} \quad \text{équivaut au système} \quad \begin{cases} 4 &= \lambda + 6\mu \\ -1 &= 2\lambda + 4\mu \\ 8 &= -\lambda + 2\mu. \end{cases}$$

Or ce système n'a aucune solution. Donc il n'existe pas $\lambda, \mu \in \mathbb{R}$ tels que $w = \lambda u + \mu v$.

4.2. Caractérisation d'un sous-espace vectoriel

Théorème 53. Caractérisation d'un sous-espace par la notion de combinaison linéaire

Soient E un $\mathbb{K}$-espace vectoriel et F une partie non vide de E. F est un sous-espace vectoriel de E si et seulement si

$$\lambda u + \mu v \in F \qquad \text{pour tous } u, v \in F \qquad \text{et tous } \lambda, \mu \in \mathbb{K}.$$

Autrement dit si et seulement si toute combinaison linéaire de deux éléments de F appartient à F.

Démonstration

- Supposons que F soit un sous-espace vectoriel. Et soient $u, v \in F$, $\lambda, \mu \in \mathbb{K}$. Alors par la définition de sous-espace vectoriel : $\lambda u \in F$ et $\mu v \in F$ et ainsi $\lambda u + \mu v \in F$.
- Réciproquement, supposons que pour chaque $u, v \in F$, $\lambda, \mu \in \mathbb{K}$ on a $\lambda u + \mu v \in F$.
  - Comme F n'est pas vide, soient $u, v \in F$. Posons $\lambda = \mu = 0$. Alors $\lambda u + \mu v = 0_E \in F$.
  - Si $u, v \in F$, alors en posant $\lambda = \mu = 1$ on obtient $u + v \in F$.

– Si $u \in F$ et $\lambda \in \mathbb{K}$ (et pour n'importe quel v, en posant $\mu = 0$), alors $\lambda u \in F$.

4.3. Intersection de deux sous-espaces vectoriels

Proposition 110. Intersection de deux sous-espaces

Soient F, G deux sous-espaces vectoriels d'un $\mathbb{K}$-espace vectoriel E. L'intersection $F \cap G$ est un sous-espace vectoriel de E.

On démontrerait de même que l'intersection $F_1 \cap F_2 \cap F_3 \cap \cdots \cap F_n$ d'une famille quelconque de sous-espaces vectoriels de E est un sous-espace vectoriel de E.

Démonstration

Soient F et G deux sous-espaces vectoriels de E.

- $0_E \in F$, $0_E \in G$ car F et G sont des sous-espaces vectoriels de E ; donc $0_E \in F \cap G$.
- Soient u et v deux vecteurs de $F \cap G$. Comme F est un sous-espace vectoriel, alors $u, v \in F$ implique $u + v \in F$. De même $u, v \in G$ implique $u + v \in G$. Donc $u + v \in F \cap G$.
- Soient $u \in F \cap G$ et $\lambda \in \mathbb{K}$. Comme F est un sous-espace vectoriel, alors $u \in F$ implique $\lambda u \in F$. De même $u \in G$ implique $\lambda u \in G$. Donc $\lambda u \in F \cap G$.

Conclusion : $F \cap G$ est un sous-espace vectoriel de E.

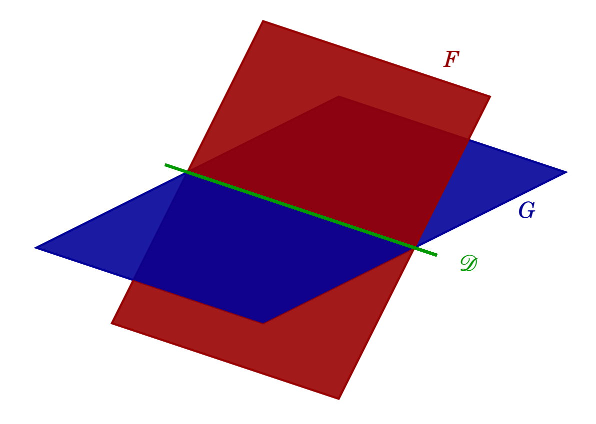
Exemple 191

Soit $\mathscr{D}$ le sous-ensemble de $\mathbb{R}^3$ défini par :

$$\mathscr{D} = \left\{(x, y, z) \in \mathbb{R}^3 \mid x + 3y + z = 0 \quad \text{et} \quad x - y + 2z = 0\right\}.$$

Est-ce que $\mathscr{D}$ est sous-espace vectoriel de $\mathbb{R}^3$? L'ensemble $\mathscr{D}$ est l'intersection de F et G, les sous-ensembles de $\mathbb{R}^3$ définis par :

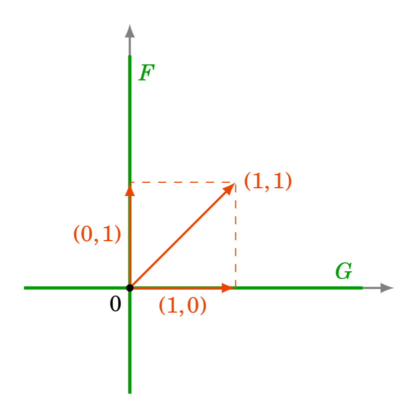
$$F = \left\{(x, y, z) \in \mathbb{R}^3 \mid x + 3y + z = 0\right\}$$
$$G = \left\{(x, y, z) \in \mathbb{R}^3 \mid x - y + 2z = 0\right\}$$



Ce sont deux plans passant par l'origine, donc des sous-espaces vectoriels de $\mathbb{R}^3$. Ainsi $\mathscr{D} = F \cap G$ est un sous-espace vectoriel de $\mathbb{R}^3$, c'est une droite vectorielle.

Remarque

La réunion de deux sous-espaces vectoriels de E n'est pas en général un sous-espace vectoriel de E. Prenons par exemple $E = \mathbb{R}^2$. Considérons les sous-espaces vectoriels $F = \{(x, y) \mid x = 0\}$ et $G = \{(x, y) \mid y = 0\}$. Alors $F \cup G$ n'est pas un sous-espace vectoriel de $\mathbb{R}^2$. Par exemple, $(0,1)+(1,0) = (1,1)$ est la somme d'un élément de F et d'un élément de G, mais n'est pas dans $F \cup G$.



4.4. Mini-exercices

1. Peut-on trouver $t \in \mathbb{R}$ tel que les vecteurs $\begin{pmatrix} -2 \\ \sqrt{2} \\ t \end{pmatrix}$ et $\begin{pmatrix} -4\sqrt{2} \\ 4t \\ 2\sqrt{2} \end{pmatrix}$ soient colinéaires ?
2. Peut-on trouver $t \in \mathbb{R}$ tel que le vecteur $\begin{pmatrix} 1 \\ 3t \\ t \end{pmatrix}$ soit une combinaison linéaire de $\begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix}$ et $\begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$?

5. Sous-espace vectoriel (fin)

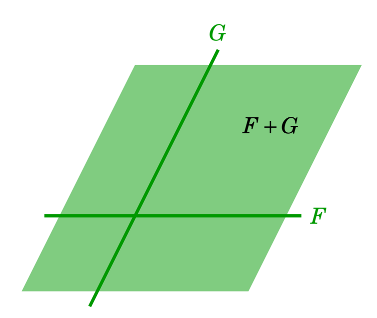
5.1. Somme de deux sous-espaces vectoriels

Comme la réunion de deux sous-espaces vectoriels F et G n'est pas en général un sous-espace vectoriel, il est utile de connaître les sous-espaces vectoriels qui contiennent à la fois les deux sous-espaces vectoriels F et G, et en particulier le plus petit d'entre eux (au sens de l'inclusion).

Définition 96. Définition de la somme de deux sous-espaces

Soient F et G deux sous-espaces vectoriels d'un $\mathbb{K}$-espace vectoriel E. L'ensemble de tous les éléments $u + v$, où u est un élément de F et v un élément de G, est appelé ***somme*** des sous-espaces vectoriels F et G. Cette somme est notée $F + G$. On a donc

$$F + G = \{u + v \mid u \in F, v \in G\}.$$



Proposition 111

Soient F et G deux sous-espaces vectoriels du $\mathbb{K}$-espace vectoriel E.

1. $F+G$ est un sous-espace vectoriel de E.
2. $F+G$ est le plus petit sous-espace vectoriel contenant à la fois F et G.

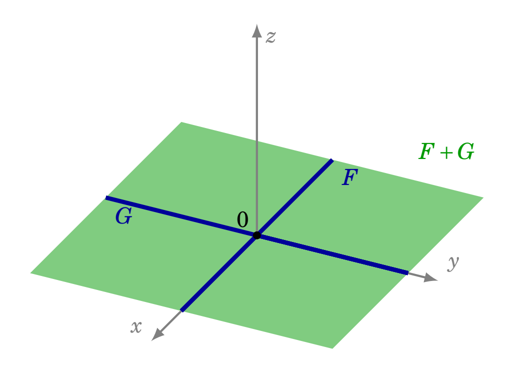
Démonstration

1. Montrons que $F+G$ est un sous-espace vectoriel.
   - $0_E \in F$, $0_E \in G$, donc $0_E = 0_E + 0_E \in F+G$.
   - Soient w et w' des éléments de $F+G$. Comme w est dans $F+G$, il existe u dans F et v dans G tels que $w = u+v$. Comme w' est dans $F+G$, il existe u' dans F et v' dans G tels que $w' = u'+v'$. Alors $w+w' = (u+v)+(u'+v') = (u+u')+(v+v') \in F+G$, car $u+u' \in F$ et $v+v' \in G$.
   - Soit w un élément de $F+G$ et $\lambda \in \mathbb{K}$. Il existe u dans F et v dans G tels que $w = u+v$. Alors $\lambda w = \lambda(u+v) = (\lambda u)+(\lambda v) \in F+G$, car $\lambda u \in F$ et $\lambda v \in G$.
2. – L'ensemble $F+G$ contient F et contient G : en effet tout élément u de F s'écrit $u = u+0$ avec u appartenant à F et 0 appartenant à G (puisque G est un sous-espace vectoriel), donc u appartient à $F+G$. De même pour un élément de G.
   - Si H est un sous-espace vectoriel contenant F et G, alors montrons que $F+G \subset H$. C'est clair : si $u \in F$ alors en particulier $u \in H$ (car $F \subset H$), de même si $v \in G$ alors $v \in H$. Comme H est un sous-espace vectoriel, alors $u+v \in H$.

Exemple 192

Déterminons $F+G$ dans le cas où F et G sont les sous-espaces vectoriels de $\mathbb{R}^3$ suivants :

$$F = \{(x,y,z) \in \mathbb{R}^3 \mid y = z = 0\} \qquad \text{et} \qquad G = \{(x,y,z) \in \mathbb{R}^3 \mid x = z = 0\}.$$

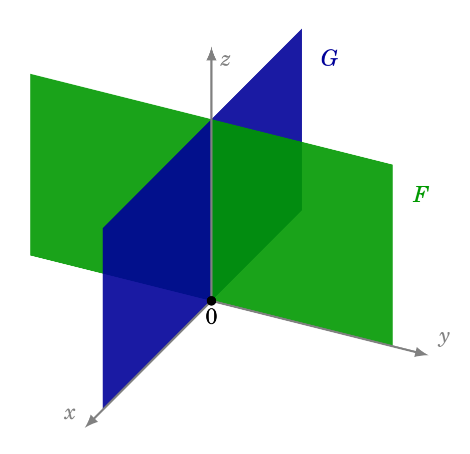


Un élément w de $F+G$ s'écrit $w = u+v$ où u est un élément de F et v un élément de G. Comme $u \in F$ alors il existe $x \in \mathbb{R}$ tel que $u = (x,0,0)$, et comme $v \in G$ il existe $y \in \mathbb{R}$ tel que $v = (0,y,0)$. Donc $w = (x,y,0)$. Réciproquement, un tel élément $w = (x,y,0)$ est la somme de $(x,0,0)$ et de $(0,y,0)$. Donc $F+G = \{(x,y,z) \in \mathbb{R}^3 \mid z = 0\}$. On voit même que, pour cet exemple, tout élément de $F+G$ s'écrit de façon *unique* comme la somme d'un élément de F et d'un élément de G.

Exemple 193

Soient F et G les deux sous-espaces vectoriels de $\mathbb{R}^3$ suivants :

$$F = \{(x,y,z) \in \mathbb{R}^3 \mid x = 0\} \qquad \text{et} \qquad G = \{(x,y,z) \in \mathbb{R}^3 \mid y = 0\}.$$



Dans cet exemple, montrons que $F+G = \mathbb{R}^3$. Par définition de $F+G$, tout élément de $F+G$ est dans $\mathbb{R}^3$. Mais réciproquement, si $w = (x,y,z)$ est un élément quelconque de $\mathbb{R}^3$: $w = (x,y,z) = (0,y,z)+(x,0,0)$, avec $(0,y,z) \in F$ et $(x,0,0) \in G$, donc w appartient à $F+G$.
Remarquons que, dans cet exemple, un élément de $\mathbb{R}^3$ ne s'écrit pas forcément de façon unique comme la somme d'un élément de F et d'un élément de G. Par exemple $(1,2,3) = (0,2,3)+(1,0,0) = (0,2,0)+(1,0,3)$.

5.2. Sous-espaces vectoriels supplémentaires

Définition 97. Définition de la somme directe de deux sous-espaces

Soient F et G deux sous-espaces vectoriels de E. F et G sont en ***somme directe*** dans E si

- $F \cap G = \{0_E\}$,
- $F+G = E$.

On note alors $F \oplus G = E$.

Si F et G sont en somme directe, on dit que F et G sont des sous-espaces vectoriels ***supplémentaires*** dans E.

Proposition 112

F et G sont supplémentaires dans E si et seulement si tout élément de E s'écrit d'une manière ***unique*** comme la somme d'un élément de F et d'un élément de G.

Remarque

- Dire qu'un élément w de E s'écrit d'une manière unique comme la somme d'un élément de F et d'un élément de G signifie que si $w = u+v$ avec $u \in F$, $v \in G$ et $w = u'+v'$ avec $u' \in F$, $v' \in G$ alors $u = u'$ et $v = v'$.
- On dit aussi que F est un sous-espace supplémentaire de G (ou que G est un sous-espace supplémentaire de F).
- Il n'y a pas unicité du supplémentaire d'un sous-espace vectoriel donné (voir un exemple ci-dessous).

– L'existence d'un supplémentaire d'un sous-espace vectoriel sera prouvée dans le cadre des espaces vectoriels de dimension finie.

Démonstration

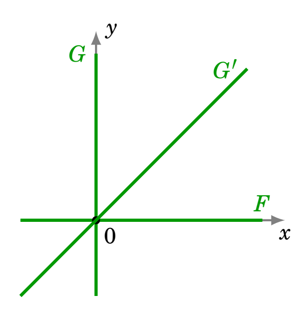
– Supposons $E = F \oplus G$ et montrons que tout élément $u \in E$ se décompose de manière unique. Soient donc $u = v + w$ et $u = v' + w'$ avec $v, v' \in F$ et $w, w' \in G$. On a alors $v + w = v' + w'$, donc $v - v' = w' - w$. Comme F est un sous-espace vectoriel alors $v - v' \in F$, mais d'autre part G est aussi un sous-espace vectoriel donc $w' - w \in G$. Conclusion : $v - v' = w' - w \in F \cap G$. Mais par définition d'espaces supplémentaires $F \cap G = \{0_E\}$, donc $v - v' = 0_E$ et aussi $w' - w = 0_E$. On en déduit $v = v'$ et $w = w'$, ce qu'il fallait démontrer.
– Supposons que tout $u \in E$ se décompose de manière unique et montrons $E = F \oplus G$.
  – Montrons $F \cap G = \{0_E\}$. Si $u \in F \cap G$, il peut s'écrire des deux manières suivantes comme somme d'un élément de F et d'un élément de G :

$$u = 0_E + u \qquad \text{et} \qquad u = u + 0_E.$$

  Par l'unicité de la décomposition, $u = 0_E$.
  – Montrons $F + G = E$. Il n'y rien à prouver, car par hypothèse tout élément u se décompose en $u = v + w$, avec $v \in F$ et $w \in G$.

Exemple 194

1. Soient $F = \{(x,0) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$ et $G = \{(0,y) \in \mathbb{R}^2 \mid y \in \mathbb{R}\}$.
   Montrons que $F \oplus G = \mathbb{R}^2$. La première façon de le voir est que l'on a clairement $F \cap G = \{(0,0)\}$ et que, comme $(x,y) = (x,0) + (0,y)$, alors $F + G = \mathbb{R}^2$. Une autre façon de le voir est d'utiliser la proposition 112, car la décomposition $(x,y) = (x,0) + (0,y)$ est unique.



2. Gardons F et notons $G' = \{(x,x) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$. Montrons que l'on a aussi $F \oplus G' = \mathbb{R}^2$:
   (a) Montrons $F \cap G' = \{(0,0)\}$. Si $(x,y) \in F \cap G'$ alors d'une part $(x,y) \in F$ donc $y = 0$, et aussi $(x,y) \in G'$ donc $x = y$. Ainsi $(x,y) = (0,0)$.
   (b) Montrons $F + G' = \mathbb{R}^2$. Soit $u = (x,y) \in \mathbb{R}^2$. Cherchons $v \in F$ et $w \in G'$ tels que $u = v + w$. Comme $v = (x_1, y_1) \in F$ alors $y_1 = 0$, et comme $w = (x_2, y_2) \in G'$ alors $x_2 = y_2$. Il s'agit donc de trouver x_1 et x_2 tels que

$$(x,y) = (x_1, 0) + (x_2, x_2).$$

   Donc $(x,y) = (x_1 + x_2, x_2)$. Ainsi $x = x_1 + x_2$ et $y = x_2$, d'où $x_1 = x - y$ et $x_2 = y$. On trouve bien

$$(x,y) = (x - y, 0) + (y, y),$$

   qui prouve que tout élément de $\mathbb{R}^2$ est somme d'un élément de F et d'un élément de G'.

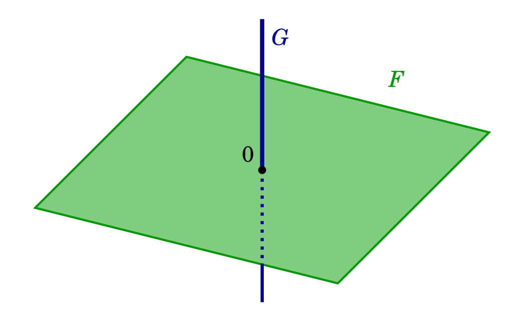
3. De façon plus générale, deux droites distinctes du plan passant par l'origine forment des sous-espaces supplémentaires.

Exemple 195

Est-ce que les sous-espaces vectoriels F et G de $\mathbb{R}^3$ définis par

$$F = \left\{(x,y,z) \in \mathbb{R}^3 \mid x - y - z = 0\right\} \qquad \text{et} \qquad G = \left\{(x,y,z) \in \mathbb{R}^3 \mid y = z = 0\right\}$$

sont supplémentaires dans $\mathbb{R}^3$?



1. Il est facile de vérifier que $F \cap G = \{0\}$. En effet si l'élément $u = (x,y,z)$ appartient à l'intersection de F et de G, alors les coordonnées de u vérifient : $x - y - z = 0$ (car u appartient à F), et $y = z = 0$ (car u appartient à G), donc $u = (0,0,0)$.
2. Il reste à démontrer que $F + G = \mathbb{R}^3$.

   Soit donc $u = (x,y,z)$ un élément quelconque de $\mathbb{R}^3$; il faut déterminer des éléments v de F et w de G tels que $u = v + w$. L'élément v doit être de la forme $v = (y_1 + z_1, y_1, z_1)$ et l'élément w de la forme $w = (x_2, 0, 0)$. On a $u = v + w$ si et seulement si $y_1 = y$, $z_1 = z$, $x_2 = x - y - z$. On a donc

$$(x,y,z) = (y+z, y, z) + (x - y - z, 0, 0)$$

   avec $v = (y+z, y, z)$ dans F et $w = (x - y - z, 0, 0)$ dans G.

Conclusion : $F \oplus G = \mathbb{R}^3$.

Exemple 196

Dans le $\mathbb{R}$-espace vectoriel $\mathscr{F}(\mathbb{R},\mathbb{R})$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, on considère le sous-espace vectoriel des fonctions paires $\mathscr{P}$ et le sous-espace vectoriel des fonctions impaires $\mathscr{I}$. Montrons que $\mathscr{P} \oplus \mathscr{I} = \mathscr{F}(\mathbb{R},\mathbb{R})$.

1. Montrons $\mathscr{P} \cap \mathscr{I} = \{0_{\mathscr{F}(\mathbb{R},\mathbb{R})}\}$.

   Soit $f \in \mathscr{P} \cap \mathscr{I}$, c'est-à-dire que f est à la fois une fonction paire et impaire. Il s'agit de montrer que f est la fonction identiquement nulle. Soit $x \in \mathbb{R}$. Comme $f(-x) = f(x)$ (car f est paire) et $f(-x) = -f(x)$ (car f est impaire), alors $f(x) = -f(x)$, ce qui implique $f(x) = 0$. Ceci est vrai quel que soit $x \in \mathbb{R}$; donc f est la fonction nulle. Ainsi $\mathscr{P} \cap \mathscr{I} = \{0_{\mathscr{F}(\mathbb{R},\mathbb{R})}\}$.
2. Montrons $\mathscr{P} + \mathscr{I} = \mathscr{F}(\mathbb{R},\mathbb{R})$.

   Soit $f \in \mathscr{F}(\mathbb{R},\mathbb{R})$. Il s'agit de montrer que f peut s'écrire comme la somme d'une fonction paire et d'une fonction impaire.

   Analyse. Si $f = g + h$, avec $g \in \mathscr{P}$, $h \in \mathscr{I}$, alors pour tout x, d'une part, (a) $f(x) = g(x) + h(x)$, et d'autre part, (b) $f(-x) = g(-x) + h(-x) = g(x) - h(x)$. Par somme et différence de (a) et

(b), on tire que

$$g(x) = \frac{f(x)+f(-x)}{2} \qquad \text{et} \qquad h(x) = \frac{f(x)-f(-x)}{2}.$$

Synthèse. Pour $f \in \mathscr{F}(\mathbb{R},\mathbb{R})$, on définit deux fonctions g, h par $g(x) = \frac{f(x)+f(-x)}{2}$ et $h(x) = \frac{f(x)-f(-x)}{2}$. Alors d'une part $f(x) = g(x)+h(x)$ et d'autre part $g \in \mathscr{P}$ (vérifier $g(-x) = g(x)$) et $h \in \mathscr{I}$ (vérifier $h(-x) = -h(x)$). Bilan : $\mathscr{P}+\mathscr{I} = \mathscr{F}(\mathbb{R},\mathbb{R})$.

En conclusion, $\mathscr{P}$ et $\mathscr{I}$ sont en somme directe dans $\mathscr{F}(\mathbb{R},\mathbb{R})$: $\mathscr{P} \oplus \mathscr{I} = \mathscr{F}(\mathbb{R},\mathbb{R})$. Notez que, comme le prouvent nos calculs, les g et h obtenus sont uniques.

5.3. Sous-espace engendré

Théorème 54. Théorème de structure de l'ensemble des combinaisons linéaires

Soit $\{v_1,\dots,v_n\}$ un ensemble fini de vecteurs d'un $\mathbb{K}$-espace vectoriel E. Alors :

- L'ensemble des combinaisons linéaires des vecteurs $\{v_1,\dots,v_n\}$ est un sous-espace vectoriel de E.
- C'est le plus petit sous-espace vectoriel de E (au sens de l'inclusion) contenant les vecteurs $v_1,\dots,v_n$.

Notation. Ce sous-espace vectoriel est appelé ***sous-espace engendré par** $v_1,\dots,v_n$* et est noté $\mathrm{Vect}(v_1,\dots,v_n)$. On a donc

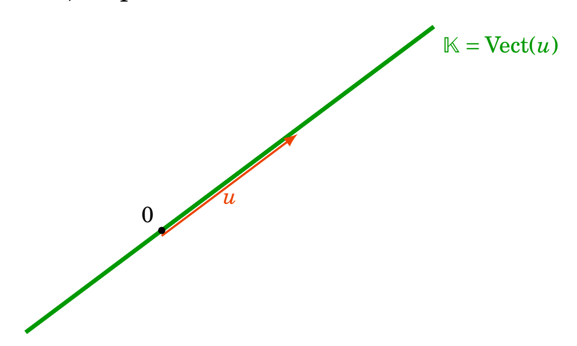
$$u \in \mathrm{Vect}(v_1,\dots,v_n) \iff \text{il existe } \lambda_1,\dots,\lambda_n \in \mathbb{K} \quad \text{tels que} \quad u = \lambda_1 v_1 + \dots + \lambda_n v_n$$

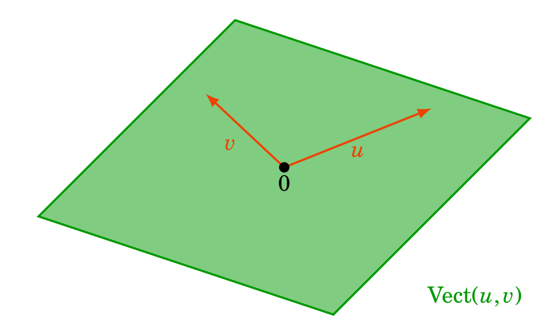
Remarque

- Dire que $\mathrm{Vect}(v_1,\dots,v_n)$ est le plus petit sous-espace vectoriel de E contenant les vecteurs $v_1,\dots,v_n$ signifie que si F est un sous-espace vectoriel de E contenant aussi les vecteurs $v_1,\dots,v_n$ alors $\mathrm{Vect}(v_1,\dots,v_n) \subset F$.
- Plus généralement, on peut définir le sous-espace vectoriel engendré par une partie $\mathcal{V}$ quelconque (non nécessairement finie) d'un espace vectoriel : $\mathrm{Vect}\,\mathcal{V}$ est le plus petit sous-espace vectoriel contenant $\mathcal{V}$.

Exemple 197

1. E étant un $\mathbb{K}$-espace vectoriel, et u un élément quelconque de E, l'ensemble $\mathrm{Vect}(u) = \{\lambda u \mid \lambda \in \mathbb{K}\}$ est le sous-espace vectoriel de E engendré par u. Il est souvent noté $\mathbb{K}u$. Si u n'est pas le vecteur nul, on parle d'une ***droite vectorielle***.





2. Si u et v sont deux vecteurs de E, alors $\mathrm{Vect}(u,v) = \{\lambda u + \mu v \mid \lambda, \mu \in \mathbb{K}\}$. Si u et v ne sont pas colinéaires, alors $\mathrm{Vect}(u,v)$ est un ***plan vectoriel***.
3. Soient $u = \begin{pmatrix}1\\1\\1\end{pmatrix}$ et $v = \begin{pmatrix}1\\2\\3\end{pmatrix}$ deux vecteurs de $\mathbb{R}^3$. Déterminons $\mathscr{P} = \mathrm{Vect}(u,v)$.

$$\begin{aligned}\begin{pmatrix}x\\y\\z\end{pmatrix} \in \mathrm{Vect}(u,v) &\iff \begin{pmatrix}x\\y\\z\end{pmatrix} = \lambda u + \mu v \quad \text{pour certains } \lambda, \mu \in \mathbb{R} \\ &\iff \begin{pmatrix}x\\y\\z\end{pmatrix} = \lambda \begin{pmatrix}1\\1\\1\end{pmatrix} + \mu \begin{pmatrix}1\\2\\3\end{pmatrix} \\ &\iff \begin{cases} x = \lambda + \mu \\ y = \lambda + 2\mu \\ z = \lambda + 3\mu \end{cases}\end{aligned}$$

Nous obtenons bien une équation paramétrique du plan $\mathscr{P}$ passant par l'origine et contenant les vecteurs u et v. On sait en trouver une équation cartésienne : $(x - 2y + z = 0)$.

Exemple 198

Soient E l'espace vectoriel des applications de $\mathbb{R}$ dans $\mathbb{R}$ et f_0, f_1, f_2 les applications définies par :

$$\forall x \in \mathbb{R} \qquad f_0(x) = 1, \; f_1(x) = x \;\text{ et }\; f_2(x) = x^2.$$

Le sous-espace vectoriel de E engendré par $\{f_0, f_1, f_2\}$ est l'espace vectoriel des fonctions polynômes f de degré inférieur ou égal à 2, c'est-à-dire de la forme $f(x) = ax^2 + bx + c$.

Méthodologie. On peut démontrer qu'une partie F d'un espace vectoriel E est un sous-espace vectoriel de E en montrant que F est égal à l'ensemble des combinaisons linéaires d'un nombre fini de vecteurs de E.

Exemple 199

Est-ce que $F = \{(x,y,z) \in \mathbb{R}^3 \mid x - y - z = 0\}$ est un sous-espace vectoriel de $\mathbb{R}^3$?
Un triplet de $\mathbb{R}^3$ est élément de F si et seulement si $x = y + z$. Donc u est élément de F si et seulement s'il peut s'écrire $u = (y + z, y, z)$. Or, on a l'égalité

$$(y + z, y, z) = y(1,1,0) + z(1,0,1).$$

Donc F est l'ensemble des combinaisons linéaires de $\{(1,1,0),(1,0,1)\}$. C'est le sous-espace vectoriel engendré par $\{(1,1,0),(1,0,1)\}$: $F = \mathrm{Vect}\{(1,1,0),(1,0,1)\}$. C'est bien un plan vectoriel (un plan passant par l'origine).

Démonstration . Preuve du théorème 54

1. On appelle F l'ensemble des combinaisons linéaires des vecteurs $\{v_1, \dots, v_n\}$.
   (a) $0_E \in F$ car F contient la combinaison linéaire particulière $0v_1 + \cdots + 0v_n$.
   (b) Si $u, v \in F$ alors il existe $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ tels que $u = \lambda_1 v_1 + \cdots + \lambda_n v_n$ et $\mu_1, \dots, \mu_n \in \mathbb{K}$ tels que $v = \mu_1 v_1 + \cdots + \mu_n v_n$. On en déduit que $u + v = (\lambda_1 + \mu_1)v_1 + \cdots + (\lambda_n + \mu_n)v_n$ appartient bien à F.
   (c) De même, $\lambda \cdot u = (\lambda\lambda_1)v_1 + \cdots + (\lambda\lambda_n)v_n \in F$.

   Conclusion : F est un sous-espace vectoriel.
2. Si G est un sous-espace vectoriel contenant $\{v_1, \dots, v_n\}$, alors il est stable par combinaison linéaire ; il contient donc toute combinaison linéaire des vecteurs $\{v_1, \dots, v_n\}$. Par conséquent F est inclus dans G : F est le plus petit sous-espace (au sens de l'inclusion) contenant $\{v_1, \dots, v_n\}$.

5.4. Mini-exercices

1. Trouver des sous-espaces vectoriels distincts F et G de $\mathbb{R}^3$ tels que
   (a) $F + G = \mathbb{R}^3$ et $F \cap G \neq \{0\}$;
   (b) $F + G \neq \mathbb{R}^3$ et $F \cap G = \{0\}$;
   (c) $F + G = \mathbb{R}^3$ et $F \cap G = \{0\}$;
   (d) $F + G \neq \mathbb{R}^3$ et $F \cap G \neq \{0\}$.
2. Soient $F = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}$ et $G = \mathrm{Vect}\{(1, 1, 1)\} \subset \mathbb{R}^3$.
   (a) Montrer que F est un espace vectoriel. Trouver deux vecteurs u, v tels que $F = \mathrm{Vect}(u, v)$.
   (b) Calculer $F \cap G$ et montrer que $F + G = \mathbb{R}^3$. Que conclure ?
3. Soient $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $C = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $D = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ des matrices de $M_2(\mathbb{R})$.
   (a) Quel est l'espace vectoriel F engendré par A et B ? Idem avec G engendré par C et D.
   (b) Calculer $F \cap G$. Montrer que $F + G = M_2(\mathbb{R})$. Conclure.

6. Application linéaire (début)

6.1. Définition

Nous avons déjà rencontré la notion d'application linéaire dans le cas $f : \mathbb{R}^p \longrightarrow \mathbb{R}^n$ (voir le chapitre « L'espace vectoriel $\mathbb{R}^n$ »). Cette notion se généralise à des espaces vectoriels quelconques.

Définition 98

Soient E et F deux $\mathbb{K}$-espaces vectoriels. Une application f de E dans F est une ***application linéaire*** si elle satisfait aux deux conditions suivantes :

1. $f(u + v) = f(u) + f(v)$, pour tous $u, v \in E$;
2. $f(\lambda \cdot u) = \lambda \cdot f(u)$, pour tout $u \in E$ et tout $\lambda \in \mathbb{K}$.

Autrement dit : une application est linéaire si elle « respecte » les deux lois d'un espace vectoriel.

Notation. L'ensemble des applications linéaires de E dans F est noté $\mathscr{L}(E, F)$.

6.2. Premiers exemples

Exemple 200

L'application f définie par

$$\begin{array}{rccc} f : & \mathbb{R}^3 & \to & \mathbb{R}^2 \\ & (x,y,z) & \mapsto & (-2x, y+3z) \end{array}$$

est une application linéaire. En effet, soient $u = (x,y,z)$ et $v = (x',y',z')$ deux éléments de $\mathbb{R}^3$ et λ un réel.

$$\begin{array}{rcl} f(u+v) & = & f(x+x', y+y', z+z') \\ & = & \big(-2(x+x'), y+y'+3(z+z')\big) \\ & = & (-2x, y+3z)+(-2x', y'+3z') \\ & = & f(u)+f(v) \end{array} \quad \text{et} \quad \begin{array}{rcl} f(\lambda \cdot u) & = & f(\lambda x, \lambda y, \lambda z) \\ & = & (-2\lambda x, \lambda y+3\lambda z) \\ & = & \lambda \cdot (-2x, y+3z) \\ & = & \lambda \cdot f(u) \end{array}$$

Toutes les applications ne sont pas des applications linéaires !

Exemple 201

Soit $f : \mathbb{R} \to \mathbb{R}$ l'application définie par $f(x) = x^2$. On a $f(1) = 1$ et $f(2) = 4$. Donc $f(2) \neq 2 \cdot f(1)$. Ce qui fait que l'on n'a pas l'égalité $f(\lambda x) = \lambda f(x)$ pour un certain choix de λ, x. Donc f n'est pas linéaire. Notez que l'on n'a pas non plus $f(x+x') = f(x)+f(x')$ dès que $xx' \neq 0$.

Voici d'autres exemples d'applications linéaires :

1. Pour une matrice fixée $A \in M_{n,p}(\mathbb{R})$, l'application $f : \mathbb{R}^p \longrightarrow \mathbb{R}^n$ définie par

$$f(X) = AX$$

   est une application linéaire.

2. L'***application nulle***, notée $0_{\mathscr{L}(E,F)}$:

$$f : E \longrightarrow F \qquad f(u) = 0_F \qquad \text{pour tout } u \in E.$$

3. L'***application identité***, notée id_E :

$$f : E \longrightarrow E \qquad f(u) = u \qquad \text{pour tout } u \in E.$$

6.3. Premières propriétés

Proposition 113

Soient E et F deux $\mathbb{K}$-espaces vectoriels. Si f est une application linéaire de E dans F, alors :

- $f(0_E) = 0_F$,
- $f(-u) = -f(u)$, pour tout $u \in E$.

Démonstration

Il suffit d'appliquer la définition de la linéarité avec $\lambda = 0$, puis avec $\lambda = -1$.

Pour démontrer qu'une application est linéaire, on peut aussi utiliser une propriété plus « concentrée », donnée par la caractérisation suivante :

Proposition 114. Caractérisation d'une application linéaire

Soient E et F deux $\mathbb{K}$-espaces vectoriels et f une application de E dans F. L'application f est linéaire si et seulement si, pour tous vecteurs u et v de E et pour tous scalaires λ et μ de $\mathbb{K}$,

$$\boxed{f(\lambda u+\mu v)=\lambda f(u)+\mu f(v).}$$

Plus généralement, une application linéaire f préserve les combinaisons linéaires : pour tous $\lambda_1,\ldots,\lambda_n \in \mathbb{K}$ et tous $v_1,\ldots,v_n \in E$, on a

$$f(\lambda_1 v_1+\cdots+\lambda_n v_n)=\lambda_1 f(v_1)+\cdots+\lambda_n f(v_n).$$

Démonstration

- Soit f une application linéaire de E dans F. Soient $u,v\in E$, $\lambda,\mu\in\mathbb{K}$. En utilisant les deux axiomes de la définition, on a

$$f(\lambda u+\mu v)=f(\lambda u)+f(\mu v)=\lambda f(u)+\mu f(v).$$

- Montrons la réciproque. Soit $f:E\to F$ une application telle que $f(\lambda u+\mu v)=\lambda f(u)+\mu f(v)$ (pour tous $u,v\in E$, $\lambda,\mu\in\mathbb{K}$). Alors, d'une part $f(u+v)=f(u)+f(v)$ (en considérant le cas particulier où $\lambda=\mu=1$), et d'autre part $f(\lambda u)=\lambda f(u)$ (cas particulier où $\mu=0$).

Vocabulaire.
Soient E et F deux $\mathbb{K}$-espaces vectoriels.

- Une application linéaire de E dans F est aussi appelée ***morphisme*** ou ***homomorphisme*** d'espaces vectoriels. L'ensemble des applications linéaires de E dans F est noté $\mathscr{L}(E,F)$.
- Une application linéaire de E dans E est appelée ***endomorphisme*** de E. L'ensemble des endomorphismes de E est noté $\mathscr{L}(E)$.

6.4. Mini-exercices

Montrer que les applications suivantes $f_i:\mathbb{R}^2\to\mathbb{R}^2$ sont linéaires. Caractériser géométriquement ces applications et faire un dessin.

1. $f_1(x,y)=(-x,-y)$;
2. $f_2(x,y)=(3x,3y)$;
3. $f_3(x,y)=(x,-y)$;
4. $f_4(x,y)=(-x,y)$;
5. $f_5(x,y)=\left(\frac{\sqrt{3}}{2}x-\frac{1}{2}y,\frac{1}{2}x+\frac{\sqrt{3}}{2}y\right)$.

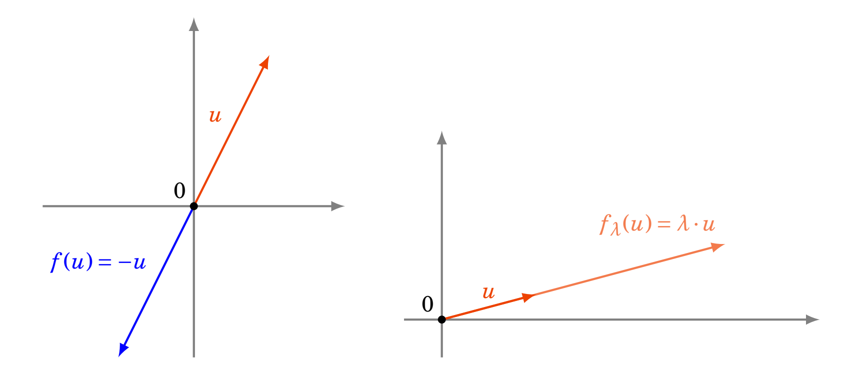
7. Application linéaire (milieu)

7.1. Exemples géométriques

Symétrie centrale.
Soient E un $\mathbb{K}$-espace vectoriel. On définit l'application f par :

$$\begin{array}{rcl} f:E & \to & E \\ u & \mapsto & -u \end{array}$$

f est linéaire et s'appelle la ***symétrie centrale*** par rapport à l'origine 0_E.



Homothétie.
Soient E un $\mathbb{K}$-espace vectoriel et $\lambda \in \mathbb{K}$. On définit l'application f_λ par :

$$\begin{array}{rcl} f_\lambda : E & \to & E \\ u & \mapsto & \lambda u \end{array}$$

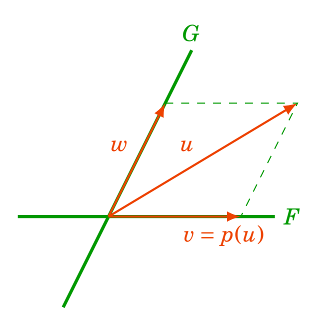
f_λ est linéaire. f_λ est appelée ***homothétie*** de rapport λ.
Cas particuliers notables :

- $\lambda = 1$, f_λ est l'application identité ;
- $\lambda = 0$, f_λ est l'application nulle ;
- $\lambda = -1$, on retrouve la symétrie centrale.

Preuve que f_λ est une application linéaire :

$$f_\lambda(\alpha u + \beta v) = \lambda(\alpha u + \beta v) = \alpha(\lambda u) + \beta(\lambda v) = \alpha f_\lambda(u) + \beta f_\lambda(v).$$

Projection.
Soient E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels supplémentaires dans E, c'est-à-dire $E = F \oplus G$. Tout vecteur u de E s'écrit de façon unique $u = v + w$ avec $v \in F$ et $w \in G$. La ***projection*** sur F parallèlement à G est l'application $p : E \to E$ définie par $p(u) = v$.



- Une projection est une application linéaire.
  En effet, soient $u, u' \in E$, $\lambda, \mu \in \mathbb{K}$. On décompose u et u' en utilisant que $E = F \oplus G$: $u = v + w$, $u' = v' + w'$ avec $v, v' \in F$, $w, w' \in G$. Commençons par écrire

  $$\lambda u + \mu u' = \lambda(v + w) + \mu(v' + w') = (\lambda v + \mu v') + (\lambda w + \mu w').$$

  Comme F et G sont des un sous-espaces vectoriels de E, alors $\lambda v + \mu v' \in F$ et $\lambda w + \mu w' \in G$. Ainsi :

  $$p(\lambda u + \mu u') = \lambda v + \mu v' = \lambda p(u) + \mu p(u').$$

- Une projection p vérifie l'égalité $p^2 = p$.
  Note : $p^2 = p$ signifie $p \circ p = p$, c'est-à-dire pour tout $u \in E$: $p\big(p(u)\big) = p(u)$. Il s'agit juste de remarquer que si $v \in F$ alors $p(v) = v$ (car $v = v + 0$, avec $v \in F$ et $0 \in G$). Maintenant, pour $u \in E$, on a $u = v + w$ avec $v \in F$ et $w \in G$. Par définition $p(u) = v$. Mais alors $p\big(p(u)\big) = p(v) = v$. Bilan : $p \circ p(u) = v = p(u)$. Donc $p \circ p = p$.

Exemple 202

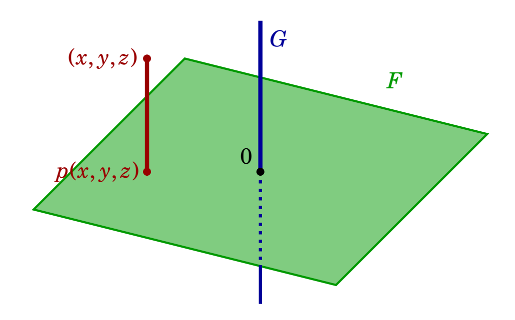
Nous avons vu que les sous-espaces vectoriels F et G de $\mathbb{R}^3$ définis par

$$F = \big\{(x,y,z) \in \mathbb{R}^3 \mid x - y - z = 0\big\} \qquad \text{et} \qquad G = \big\{(x,y,z) \in \mathbb{R}^3 \mid y = z = 0\big\}$$

sont supplémentaires dans $\mathbb{R}^3$: $\mathbb{R}^3 = F \oplus G$ (exemple 195). Nous avions vu que la décomposition s'écrivait :

$$(x,y,z) = (y+z, y, z) + (x - y - z, 0, 0).$$

Si p est la projection sur F parallèlement à G, alors on a $p(x,y,z) = (y+z, y, z)$.



Exemple 203

Nous avons vu dans l'exemple 196 que l'ensemble des fonctions paires $\mathscr{P}$ et l'ensemble des fonctions impaires $\mathscr{I}$ sont des sous-espaces vectoriels supplémentaires dans $\mathscr{F}(\mathbb{R},\mathbb{R})$. Notons p la projection sur $\mathscr{P}$ parallèlement à $\mathscr{I}$. Si f est un élément de $\mathscr{F}(\mathbb{R},\mathbb{R})$, on a $p(f) = g$ où

$$\begin{array}{rcl} g : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \dfrac{f(x) + f(-x)}{2}. \end{array}$$

7.2. Autres exemples

1. La **dérivation**. Soient $E = \mathscr{C}^1(\mathbb{R},\mathbb{R})$ l'espace vectoriel des fonctions $f : \mathbb{R} \longrightarrow \mathbb{R}$ dérivables avec f' continue et $F = \mathscr{C}^0(\mathbb{R},\mathbb{R})$ l'espace vectoriel des fonctions continues. Soit

$$\begin{array}{rcl} d : \mathscr{C}^1(\mathbb{R},\mathbb{R}) & \longrightarrow & \mathscr{C}^0(\mathbb{R},\mathbb{R}) \\ f & \longmapsto & f' \end{array}$$

   Alors d est une application linéaire, car $(\lambda f + \mu g)' = \lambda f' + \mu g'$ et donc $d(\lambda f + \mu g) = \lambda d(f) + \mu d(g)$.

2. L'**intégration**. Soient $E = \mathscr{C}^0(\mathbb{R},\mathbb{R})$ et $F = \mathscr{C}^1(\mathbb{R},\mathbb{R})$. Soit

$$\begin{array}{rcl} I : \mathscr{C}^0(\mathbb{R},\mathbb{R}) & \longrightarrow & \mathscr{C}^1(\mathbb{R},\mathbb{R}) \\ f(x) & \longmapsto & \int_0^x f(t)\,dt \end{array}$$

   L'application I est linéaire car $\int_0^x \big(\lambda f(t) + \mu g(t)\big)\,dt = \lambda \int_0^x f(t)\,dt + \mu \int_0^x g(t)\,dt$ pour toutes fonctions f et g et pour tous $\lambda, \mu \in \mathbb{R}$.

3. Avec les **polynômes**.
Soit $E = \mathbb{R}_n[X]$ l'espace vectoriel des polynômes de degré $\leqslant n$. Soit $F = \mathbb{R}_{n+1}[X]$ et soit

$$\begin{array}{rcl} f: \quad E & \longrightarrow & F \\ P(X) & \longmapsto & XP(X) \end{array}$$

Autrement dit, si $P(X) = a_n X^n + \cdots + a_1 X + a_0$, alors $f(P(X)) = a_n X^{n+1} + \cdots + a_1 X^2 + a_0 X$.
C'est une application linéaire : $f(\lambda P(X) + \mu Q(X)) = \lambda XP(X) + \mu XQ(X) = \lambda f(P(X)) + \mu f(Q(X))$.
4. La **transposition**.
Considérons l'application T de $M_n(\mathbb{K})$ dans $M_n(\mathbb{K})$ donnée par la transposition :

$$\begin{array}{rcl} T: M_n(\mathbb{K}) & \longrightarrow & M_n(\mathbb{K}) \\ A & \longmapsto & A^T \end{array}$$

T est linéaire, car on sait que pour toutes matrices $A, B \in M_n(\mathbb{K})$ et tous scalaires $\lambda, \mu \in \mathbb{K}$:

$$(\lambda A + \mu B)^T = (\lambda A)^T + (\mu B)^T = \lambda A^T + \mu B^T.$$

5. La **trace**.

$$\begin{array}{rcl} \mathrm{tr}: M_n(\mathbb{K}) & \longrightarrow & \mathbb{K} \\ A & \longmapsto & \mathrm{tr}\, A \end{array}$$

est une application linéaire car $\mathrm{tr}(\lambda A + \mu B) = \lambda \,\mathrm{tr}\, A + \mu \,\mathrm{tr}\, B$.

7.3. Mini-exercices

1. Les applications suivantes sont-elles linéaires ?
(a) $\mathbb{R} \longrightarrow \mathbb{R}, \quad x \longmapsto 3x - 2$
(b) $\mathbb{R}^4 \longrightarrow \mathbb{R}, \quad (x, y, x', y') \longmapsto x \cdot x' + y \cdot y'$
(c) $\mathscr{C}^0(\mathbb{R}, \mathbb{R}) \longrightarrow \mathbb{R}, \quad f \longmapsto f(1)$
(d) $\mathscr{C}^1(\mathbb{R}, \mathbb{R}) \longrightarrow \mathscr{C}^0(\mathbb{R}, \mathbb{R}), \quad f \longmapsto f' + f$
(e) $\mathscr{C}^0([0,1], \mathbb{R}) \longrightarrow \mathbb{R}, \quad f \longmapsto \int_0^1 |f(t)|\, dt$
(f) $\mathscr{C}^0([0,1], \mathbb{R}) \longrightarrow \mathbb{R}, \quad f \longmapsto \max_{x \in [0,1]} f(x)$
(g) $\mathbb{R}_3[X] \longrightarrow \mathbb{R}_3[X], \quad P(X) \longmapsto P(X+1) - P(0)$
2. Soient $f, g : M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R})$ définies par $A \longmapsto \frac{A + A^T}{2}$ et $A \longmapsto \frac{A - A^T}{2}$. Montrer que f et g sont des applications linéaires. Montrer que $f(A)$ est une matrice symétrique, $g(A)$ une matrice antisymétrique et que $A = f(A) + g(A)$. En déduire que les matrices symétriques et les matrices antisymétriques sont en somme directe dans $M_n(\mathbb{R})$. Caractériser géométriquement f et g.

8. Application linéaire (fin)

8.1. Image d'une application linéaire

Commençons par des rappels. Soient E et F deux ensembles et f une application de E dans F. Soit A un sous-ensemble de E. L'ensemble des images par f des éléments de A, appelé ***image directe*** de A par f, est noté $f(A)$. C'est un sous-ensemble de F. On a par définition :

$$f(A) = \{ f(x) \mid x \in A \}.$$

Dans toute la suite, E et F désigneront des $\mathbb{K}$-espaces vectoriels et $f : E \to F$ sera une application linéaire.
$f(E)$ s'appelle l'***image*** de l'application linéaire f et est noté $\operatorname{Im} f$.

Proposition 115. Structure de l'image d'un sous-espace vectoriel

1. Si E' est un sous-espace vectoriel de E, alors $f(E')$ est un sous-espace vectoriel de F.
2. En particulier, $\operatorname{Im} f$ est un sous-espace vectoriel de F.

Remarque

On a par définition de l'image directe $f(E)$:

$$f \text{ est surjective si et seulement si } \operatorname{Im} f = F.$$

Démonstration

Tout d'abord, comme $0_E \in E'$ alors $0_F = f(0_E) \in f(E')$. Ensuite on montre que pour tout couple (y_1, y_2) d'éléments de $f(E')$ et pour tous scalaires λ, μ, l'élément $\lambda y_1 + \mu y_2$ appartient à $f(E')$. En effet :

$$y_1 \in f(E') \iff \exists x_1 \in E', f(x_1) = y_1$$
$$y_2 \in f(E') \iff \exists x_2 \in E', f(x_2) = y_2.$$

Comme f est linéaire, on a

$$\lambda y_1 + \mu y_2 = \lambda f(x_1) + \mu f(x_2) = f(\lambda x_1 + \mu x_2).$$

Or $\lambda x_1 + \mu x_2$ est un élément de E', car E' est un sous-espace vectoriel de E, donc $\lambda y_1 + \mu y_2$ est bien un élément de $f(E')$.

8.2. Noyau d'une application linéaire

Définition 99. Définition du noyau

Soient E et F deux $\mathbb{K}$-espaces vectoriels et f une application linéaire de E dans F. Le ***noyau*** de f, noté $\operatorname{Ker}(f)$, est l'ensemble des éléments de E dont l'image est 0_F :

$$\boxed{\operatorname{Ker}(f) = \left\{x \in E \mid f(x) = 0_F\right\}}$$

Autrement dit, le noyau est l'image réciproque du vecteur nul de l'espace d'arrivée : $\operatorname{Ker}(f) = f^{-1}\{0_F\}$.

Proposition 116

Soient E et F deux $\mathbb{K}$-espaces vectoriels et f une application linéaire de E dans F. Le noyau de f est un sous-espace vectoriel de E.

Démonstration

$\mathrm{Ker}(f)$ est non vide car $f(0_E) = 0_F$ donc $0_E \in \mathrm{Ker}(f)$. Soient $x_1, x_2 \in \mathrm{Ker}(f)$ et $\lambda, \mu \in \mathbb{K}$. Montrons que $\lambda x_1 + \mu x_2$ est un élément de $\mathrm{Ker}(f)$. On a, en utilisant la linéarité de f et le fait que x_1 et x_2 sont des éléments de $\mathrm{Ker}(f)$: $f(\lambda x_1 + \mu x_2) = \lambda f(x_1) + \mu f(x_2) = \lambda 0_F + \mu 0_F = 0_F$.

Exemple 204

Reprenons l'exemple de l'application linéaire f définie par

$$\begin{array}{rccc} f: & \mathbb{R}^3 & \to & \mathbb{R}^2 \\ & (x,y,z) & \mapsto & (-2x, y+3z) \end{array}$$

- Calculons le noyau $\mathrm{Ker}(f)$.

$$\begin{aligned} (x,y,z) \in \mathrm{Ker}(f) & \iff f(x,y,z) = (0,0) \\ & \iff (-2x, y+3z) = (0,0) \\ & \iff \left\{ \begin{array}{rcl} -2x & = & 0 \\ y+3z & = & 0 \end{array} \right. \\ & \iff (x,y,z) = (0,-3z,z), \quad z \in \mathbb{R} \end{aligned}$$

  Donc $\mathrm{Ker}(f) = \{(0,-3z,z) \mid z \in \mathbb{R}\}$. Autrement dit, $\mathrm{Ker}(f) = \mathrm{Vect}\{(0,-3,1)\}$: c'est une droite vectorielle.
- Calculons l'image de f. Fixons $(x', y') \in \mathbb{R}^2$.

$$\begin{aligned} (x', y') = f(x,y,z) & \iff (-2x, y+3z) = (x', y') \\ & \iff \left\{ \begin{array}{rcl} -2x & = & x' \\ y+3z & = & y' \end{array} \right. \end{aligned}$$

  On peut prendre par exemple $x = -\frac{x'}{2}$, $y' = y$, $z = 0$. Conclusion : pour n'importe quel $(x', y') \in \mathbb{R}^2$, on a $f(-\frac{x'}{2}, y', 0) = (x', y')$. Donc $\mathrm{Im}(f) = \mathbb{R}^2$, et f est surjective.

Exemple 205

Soit $A \in M_{n,p}(\mathbb{R})$. Soit $f : \mathbb{R}^p \longrightarrow \mathbb{R}^n$ l'application linéaire définie par $f(X) = AX$. Alors $\mathrm{Ker}(f) = \{X \in \mathbb{R}^p \mid AX = 0\}$: c'est donc l'ensemble des $X \in \mathbb{R}^p$ solutions du système linéaire homogène $AX = 0$. On verra plus tard que $\mathrm{Im}(f)$ est l'espace engendré par les colonnes de la matrice A.

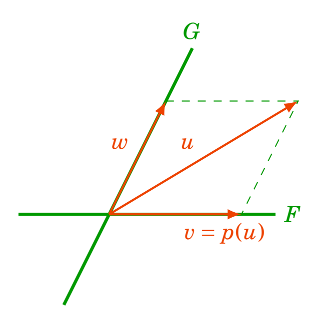
Le noyau fournit une nouvelle façon d'obtenir des sous-espaces vectoriels.

Exemple 206

Un plan $\mathscr{P}$ passant par l'origine, d'équation $(ax + by + cz = 0)$, est un sous-espace vectoriel de $\mathbb{R}^3$. En effet, soit $f : \mathbb{R}^3 \to \mathbb{R}$ l'application définie par $f(x,y,z) = ax + by + cz$. Il est facile de vérifier que f est linéaire, de sorte que $\mathrm{Ker} f = \{(x,y,z) \in \mathbb{R}^3 \mid ax + by + cz = 0\} = \mathscr{P}$ est un sous-espace vectoriel.

Exemple 207

Soient E un $\mathbb{K}$-espace vectoriel, F et G deux sous-espaces vectoriels de E, supplémentaires : $E = F \oplus G$. Soit p la projection sur F parallèlement à G. Déterminons le noyau et l'image de p.



Un vecteur u de E s'écrit d'une manière unique $u = v + w$ avec $v \in F$ et $w \in G$ et par définition $p(u) = v$.

- $\mathrm{Ker}(p) = G$: le noyau de p est l'ensemble des vecteurs u de E tels que $v = 0$, c'est donc G.
- $\mathrm{Im}(p) = F$. Il est immédiat que $\mathrm{Im}(p) \subset F$. Réciproquement, si $u \in F$ alors $p(u) = u$, donc $F \subset \mathrm{Im}(p)$.

Conclusion :

$$\mathrm{Ker}(p) = G \qquad \text{et} \qquad \mathrm{Im}(p) = F.$$

Théorème 55. Caractérisation des applications linéaires injectives

Soient E et F deux $\mathbb{K}$-espaces vectoriels et f une application linéaire de E dans F. Alors :

$$\boxed{f \text{ injective} \quad \Longleftrightarrow \quad \mathrm{Ker}(f) = \{0_E\}}$$

Autrement dit, f est injective si et seulement si son noyau ne contient que le vecteur nul. En particulier, pour montrer que f est injective, il suffit de vérifier que :

$$\text{si } f(x) = 0_F \text{ alors } x = 0_E.$$

Démonstration

- Supposons que f soit injective et montrons que $\mathrm{Ker}(f) = \{0_E\}$. Soit x un élément de $\mathrm{Ker}(f)$. On a $f(x) = 0_F$. Or, comme f est linéaire, on a aussi $f(0_E) = 0_F$. De l'égalité $f(x) = f(0_E)$, on déduit $x = 0_E$ car f est injective. Donc $\mathrm{Ker}(f) = \{0_E\}$.
- Réciproquement, supposons maintenant que $\mathrm{Ker}(f) = \{0_E\}$. Soient x et y deux éléments de E tels que $f(x) = f(y)$. On a donc $f(x) - f(y) = 0_F$. Comme f est linéaire, on en déduit $f(x-y) = 0_F$, c'est-à-dire $x - y$ est un élément de $\mathrm{Ker}(f)$. Donc $x - y = 0_E$, soit $x = y$.

Exemple 208

Considérons, pour $n \geqslant 1$, l'application linéaire

$$\begin{aligned} f : \mathbb{R}_n[X] &\longrightarrow \mathbb{R}_{n+1}[X] \\ P(X) &\longmapsto X \cdot P(X). \end{aligned}$$

Étudions d'abord le noyau de f : soit $P(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{R}_n[X]$ tel que $X \cdot P(X) = 0$.

Alors
$$a_nX^{n+1}+\cdots+a_1X^2+a_0X=0.$$
Ainsi, $a_i=0$ pour tout $i\in\{0,\ldots,n\}$ et donc $P(X)=0$. Le noyau de f est donc nul : $\mathrm{Ker}(f)=\{0\}$.
L'espace $\mathrm{Im}(f)$ est l'ensemble des polynômes de $\mathbb{R}_{n+1}[X]$ sans terme constant : $\mathrm{Im}(f)=\mathrm{Vect}\{X,X^2,\ldots,X^{n+1}\}$.
Conclusion : f est injective, mais n'est pas surjective.

8.3. L'espace vectoriel $\mathscr{L}(E,F)$

Soient E et F deux $\mathbb{K}$-espaces vectoriels. Remarquons tout d'abord que, similairement à l'exemple 181, l'ensemble des applications de E dans F, noté $\mathscr{F}(E,F)$, peut être muni d'une loi de composition interne + et d'une loi de composition externe, définies de la façon suivante : f,g étant deux éléments de $\mathscr{F}(E,F)$, et λ étant un élément de $\mathbb{K}$, pour tout vecteur u de E,

$$(f+g)(u)=f(u)+g(u) \qquad \text{et} \qquad (\lambda\cdot f)(u)=\lambda f(u).$$

Proposition 117

L'ensemble des applications linéaires entre deux $\mathbb{K}$-espaces vectoriels E et F, noté $\mathscr{L}(E,F)$, muni des deux lois définies précédemment, est un $\mathbb{K}$-espace vectoriel.

Démonstration

L'ensemble $\mathscr{L}(E,F)$ est inclus dans le $\mathbb{K}$-espace vectoriel $\mathscr{F}(E,F)$. Pour montrer que $\mathscr{L}(E,F)$ est un $\mathbb{K}$-espace vectoriel, il suffit donc de montrer que $\mathscr{L}(E,F)$ est un sous-espace vectoriel de $\mathscr{F}(E,F)$:

- Tout d'abord, l'application nulle appartient à $\mathscr{L}(E,F)$.
- Soient $f,g\in\mathscr{L}(E,F)$, et montrons que $f+g$ est linéaire. Pour tous vecteurs u et v de E et pour tous scalaires α, β de $\mathbb{K}$,

$$\begin{aligned}(f+g)(\alpha u+\beta v) &= f(\alpha u+\beta v)+g(\alpha u+\beta v) && \text{(définition de } f+g)\\ &= \alpha f(u)+\beta f(v)+\alpha g(u)+\beta g(v) && \text{(linéarité de } f \text{ et } g)\\ &= \alpha\left(f(u)+g(u)\right)+\beta\left(f(v)+g(v)\right) && \text{(propriétés des lois de } F)\\ &= \alpha(f+g)(u)+\beta(f+g)(v) && \text{(définition de } f+g)\end{aligned}$$

  $f+g$ est donc linéaire et $\mathscr{L}(E,F)$ est stable pour l'addition.
- Soient $f\in\mathscr{L}(E,F)$, $\lambda\in\mathbb{K}$, et montrons que λf est linéaire.

$$\begin{aligned}(\lambda f)(\alpha u+\beta v) &= \lambda f(\alpha u+\beta v) && \text{(définition de } \lambda f)\\ &= \lambda\big(\alpha f(u)+\beta f(v)\big) && \text{(linéarité de } f)\\ &= \alpha\lambda f(u)+\beta\lambda f(v) && \text{(propriétés des lois de } F)\\ &= \alpha(\lambda f)(u)+\beta(\lambda f)(v) && \text{(définition de } \lambda f)\end{aligned}$$

  λf est donc linéaire et $\mathscr{L}(E,F)$ est stable pour la loi externe.

$\mathscr{L}(E,F)$ est donc un sous-espace vectoriel de $\mathscr{F}(E,F)$.

En particulier, $\mathscr{L}(E)$ est un sous-espace vectoriel de $\mathscr{F}(E,E)$.

8.4. Composition et inverse d'applications linéaires

Proposition 118. Composée de deux applications linéaires

Soient E, F, G trois $\mathbb{K}$-espaces vectoriels, f une application linéaire de E dans F et g une application linéaire de F dans G. Alors $g \circ f$ est une application linéaire de E dans G.

Remarque

En particulier, le composé de deux endomorphismes de E est un endomorphisme de E. Autrement dit, $\circ$ est une loi de composition interne sur $\mathscr{L}(E)$.

Démonstration

Soient u et v deux vecteurs de E, et α et β deux éléments de $\mathbb{K}$. Alors :

$$\begin{aligned}
(g \circ f)(\alpha u + \beta v) &= g\big(f(\alpha u + \beta v)\big) && \text{(définition de } g \circ f\text{)} \\
&= g\big(\alpha f(u) + \beta f(v)\big) && \text{(linéarité de } f\text{)} \\
&= \alpha g(f(u)) + \beta g(f(v)) && \text{(linéarité de } g\text{)} \\
&= \alpha (g \circ f)(u) + \beta (g \circ f)(v) && \text{(définition de } g \circ f\text{)}
\end{aligned}$$

La composition des applications linéaires se comporte bien :

$$g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2 \qquad (g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f \qquad (\lambda g) \circ f = g \circ (\lambda f) = \lambda (g \circ f)$$

Vocabulaire.
Soient E et F deux $\mathbb{K}$-espaces vectoriels.

- Une application linéaire ***bijective*** de E sur F est appelée ***isomorphisme*** d'espaces vectoriels. Les deux espaces vectoriels E et F sont alors dits ***isomorphes***.
- Un endomorphisme bijectif de E (c'est-à-dire une application linéaire bijective de E dans E) est appelé ***automorphisme*** de E. L'ensemble des automorphismes de E est noté $GL(E)$.

Proposition 119. Linéarité de l'application réciproque d'un isomorphisme

Soient E et F deux $\mathbb{K}$-espaces vectoriels. Si f est un isomorphisme de E sur F, alors f^{-1} est un isomorphisme de F sur E.

Démonstration

Comme f est une application bijective de E sur F, alors f^{-1} est une application bijective de F sur E. Il reste donc à prouver que f^{-1} est bien linéaire. Soient u' et v' deux vecteurs de F et soient α et β deux éléments de $\mathbb{K}$. On pose $f^{-1}(u') = u$ et $f^{-1}(v') = v$, et on a alors $f(u) = u'$ et $f(v) = v'$. Comme f est linéaire, on a

$$f^{-1}(\alpha u' + \beta v') = f^{-1}\big(\alpha f(u) + \beta f(v)\big) = f^{-1}\big(f(\alpha u + \beta v)\big) = \alpha u + \beta v$$

car $f^{-1} \circ f = \mathrm{id}_E$ (où id_E désigne l'application identité de E dans E). Ainsi

$$f^{-1}(\alpha u' + \beta v') = \alpha f^{-1}(u') + \beta f^{-1}(v'),$$

et f^{-1} est donc linéaire.

Exemple 209

Soit $f:\mathbb{R}^2 \to \mathbb{R}^2$ définie par $f(x,y)=(2x+3y,x+y)$. Il est facile de prouver que f est linéaire. Pour prouver que f est bijective, on pourrait calculer son noyau et son image. Mais ici nous allons calculer directement son inverse : on cherche à résoudre $f(x,y)=(x',y')$. Cela correspond à l'équation $(2x+3y,x+y)=(x',y')$ qui est un système linéaire à deux équations et deux inconnues. On trouve $(x,y)=(-x'+3y',x'-2y')$. On pose donc $f^{-1}(x',y')=(-x'+3y',x'-2y')$. On vérifie aisément que f^{-1} est l'inverse de f, et on remarque que f^{-1} est une application linéaire.

Exemple 210

Plus généralement, soit $f:\mathbb{R}^n \to \mathbb{R}^n$ l'application linéaire définie par $f(X)=AX$ (où A est une matrice de $M_n(\mathbb{R})$). Si la matrice A est inversible, alors f^{-1} est une application linéaire bijective et est définie par $f^{-1}(X)=A^{-1}X$.
Dans l'exemple précédent,

$$X=\begin{pmatrix} x \\ y \end{pmatrix} \qquad A=\begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix} \qquad A^{-1}=\begin{pmatrix} -1 & 3 \\ 1 & -2 \end{pmatrix}.$$

8.5. Mini-exercices

1. Soit $f:\mathbb{R}^3 \to \mathbb{R}^3$ définie par $f(x,y,z)=(-x,y+z,2z)$. Montrer que f est une application linéaire. Calculer $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$. f admet-elle un inverse ? Même question avec $f(x,y,z)=(x-y,x+y,y)$.
2. Soient E un espace vectoriel, et F,G deux sous-espaces tels que $E=F\oplus G$. Chaque $u\in E$ se décompose de manière unique $u=v+w$ avec $v\in F$, $w\in G$. La ***symétrie*** par rapport à F parallèlement à G est l'application $s:E\to E$ définie par $s(u)=v-w$. Faire un dessin. Montrer que s est une application linéaire. Montrer que $s^2=\mathrm{id}_E$. Calculer $\mathrm{Ker}(s)$ et $\mathrm{Im}(s)$. s admet-elle un inverse ?
3. Soit $f:\mathbb{R}_n[X]\to\mathbb{R}_n[X]$ définie par $P(X)\mapsto P''(X)$ (où P'' désigne la dérivée seconde). Montrer que f est une application linéaire. Calculer $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$. f admet-elle un inverse ?

Auteurs

- D'après un cours de Sophie Chemla de l'université Pierre et Marie Curie, reprenant des parties d'un cours de H. Ledret et d'une équipe de l'université de Bordeaux animée par J. Queyrut,
- et un cours de Eva Bayer-Fluckiger, Philippe Chabloz, Lara Thomas de l'École Polytechnique Fédérale de Lausanne,
- mixés et révisés par Arnaud Bodin, relu par Vianney Combet.



18 Algorithmes et mathématiques

Vidéo ■ partie 1. Premiers pas avec Python
Vidéo ■ partie 2. Ecriture des entiers
Vidéo ■ partie 3. Calculs de sinus, cosinus, tangente
Vidéo ■ partie 4. Les réels
Vidéo ■ partie 5. Arithmétique - Algorithmes récursifs
Vidéo ■ partie 6. Polynômes - Complexité d'un algorithme

1. Premiers pas avec Python

Dans cette partie on vérifie d'abord que Python fonctionne, puis on introduira les boucles (for et while), le test if ... else ... et les fonctions.

1.1. Hello world !

Pour commencer testons si tout fonctionne !

Travaux pratiques 1

1. Définir deux variables prenant les valeurs 3 et 6.
2. Calculer leur somme et leur produit.

Voici à quoi cela ressemble :

Algorithme . hello-world.py

```
>>> a=3
>>> b=6
>>> somme = a+b
>>> print(somme)
9
>>> # Les résultats
>>> print("La␣somme␣est", somme)
La somme est 9
>>> produit = a*b
>>> print("Le␣produit␣est", produit)
Le produit est 18
```

On retient les choses suivantes :
- On affecte une valeur à une variable par le signe égal =.
- On affiche un message avec la fonction `print()`.
- Lorsque qu'une ligne contient un dièse #, tout ce qui suit est ignoré. Cela permet d'insérer des commentaires, ce qui est essentiel pour relire le code.

Dans la suite on omettra les symboles >>>. Voir plus de détails sur le fonctionnement en fin de section.

1.2. Somme des cubes

Travaux pratiques 2

1. Pour un entier n fixé, programmer le calcul de la somme $S_n = 1^3 + 2^3 + 3^3 + \cdots + n^3$.
2. Définir une fonction qui pour une valeur n renvoie la somme $\Sigma_n = 1 + 2 + 3 + \cdots + n$.
3. Définir une fonction qui pour une valeur n renvoie S_n.
4. Vérifier, pour les premiers entiers, que $S_n = (\Sigma_n)^2$.

1. **Algorithme . somme-cubes.py (1)**

```
n = 10
somme = 0
for i in range(1,n+1) :
    somme = somme + i*i*i
print(somme)
```

Voici ce que l'on fait pour calculer S_n avec $n = 10$.
- On affecte d'abord la valeur 0 à la variable `somme`, cela correspond à l'initialisation $S_0 = 0$.
- Nous avons défini une ***boucle*** avec l'instruction *`for`* qui fait varier i entre 1 et n.
- Nous calculons successivement S_1, S_2,... en utilisant la formule de récurrence $S_i = S_{i-1} + i^3$. Comme nous n'avons pas besoin de conserver toutes les valeurs des S_i alors on garde le même nom pour toutes les sommes, à chaque étape on affecte à `somme` l'ancienne valeur de la somme plus i^3 : `somme = somme + i*i*i`.
- `range(1,n+1)` est l'ensemble des entiers $\{1,2,\ldots,n\}$. C'est bien les entiers **strictement inférieurs à** $n+1$. La raison est que `range(n)` désigne $\{0,1,2,\ldots,n-1\}$ qui contient n éléments.

2. Nous savons que $\Sigma_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ donc nous n'avons pas besoin de faire une boucle :

Algorithme . somme-cubes.py (2)

```
def somme_entiers(n) :
    return n*(n+1)/2
```

Une ***fonction*** en informatique est similaire à une fonction mathématique, c'est un objet qui prend en entrée des variables (dites variables formelles ou variables muettes, ici n) et retourne une valeur (un entier, une liste, une chaîne de caractères,... ici $\frac{n(n+1)}{2}$).

3. Voici la fonction qui retourne la somme des cubes :

Algorithme . somme-cubes.py (3)

```
def somme_cubes(n) :
    somme = 0
    for i in range(1,n+1) :
        somme = somme + i**3
    return somme
```

4. Et enfin on vérifie que pour les premiers entiers $S_n = \left(\frac{n(n+1)}{2}\right)^2$, par exemple pour $n = 12$:

Algorithme . somme-cubes.py (4)

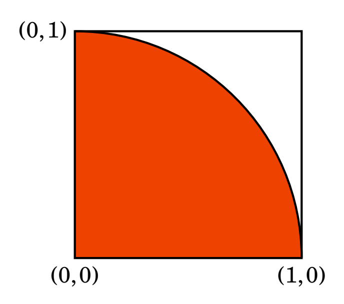
```
n = 12
if somme_cubes(n) == (somme_entiers(n)**2) :
    print("Pour n=", n, "l'assertion est vraie.")
else :
    print("L'assertion est fausse !")
```

On retient :

- Les puissances se calculent aussi avec `**` : 5^2 s'écrit `5*5` ou `5**2`, 5^3 s'écrit `5*5*5` ou `5**3`,...
- Une fonction se définit par `def ma_fonction(variable) :` et se termine par `return resultat`.
- *`if condition : ... else : ...`* exécute le premier bloc d'instructions si la condition est vraie ; si la condition est fausse cela exécute l'autre bloc.
- Exemple de conditions
  - `a < b` : $a < b$,
  - `a <= b` : $a \leqslant b$,
  - `a == b` : $a = b$,
  - `a=b!` : $a \neq b$.
- Attention ! Il est important de comprendre que `a==b` vaut soit vraie ou faux (on compare a et b) alors qu'avec `a=b` on affecte dans a la valeur de b.
- Enfin en `Python` (contrairement aux autres langages) c'est l'indentation (les espaces en début de chaque ligne) qui détermine les blocs d'instructions.

1.3. Calcul de π au hasard

Nous allons voir qu'il est possible de calculer les premières décimales de π par la méthode de Monte-Carlo, c'est à dire avec l'aide du hasard. On considère le carré de coté 1, le cercle de rayon 1 centré à l'origine, d'équation $x^2 + y^2 = 1$, et la portion de disque dans le carré (voir la figure).



Travaux pratiques 3

1. Calculer l'aire du carré et de la portion de disque.
2. Pour un point (x, y) tiré au hasard dans le carré, quelle est la probabilité que le point soit en fait dans la portion de disque ?
3. Tirer un grand nombre de points au hasard, compter ceux qui sont dans la portion de disque.
4. En déduire les premières décimales de π.

Voici le code :

Algorithme . pi-hasard.py

```
import random              # Module qui génère des nombres aléatoires

Tir = 0                    # Numéro du tir
NbTirDansLeDisque = 0      # Nombre de tirs dans le disque

while (Tir < 1000) :
    Tir = Tir + 1
    # On tire au hasard un point (x,y) dans [0,1] x [0,1]
    x = random.random()
    y = random.random()
    if (x*x+y*y <= 1) :    # On est dans le disque
        NbTirDansLeDisque = NbTirDansLeDisque + 1

MonPi = 4*NbTirDansLeDisque / Tir
print("Valeur expérimentale de Pi : %0.3f" %MonPi)
```

Commentaires :

- Un petit calcul prouve que l'aire de la portion de disque est $\frac{\pi}{4}$, l'aire du carré est 1. Donc la probabilité de tomber dans le disque est $\frac{\pi}{4}$.
- Pour tirer un nombre au hasard on utilise une fonction `random()` qui renvoie un nombre réel de l'intervalle $[0, 1[$. Bien sûr à chaque appel de la fonction `random()` le nombre obtenu est différent !
- Cette fonction n'est pas connue par défaut de `Python`, il faut lui indiquer le nom du ***module*** où elle se trouve. En début de fichier on ajoute `import random` pour le module qui gère les tirages au hasard. Et pour indiquer qu'une fonction vient d'un module il faut l'appeler par

module.fonction() donc ici random.random() (module et fonction portent ici le même nom !).

- La boucle est *while condition : ...* Tant que la condition est vérifiée les instructions de la boucle sont exécutées. Ici Tir est le compteur que l'on a initialisé à 0. Ensuite on commence à exécuter la boucle. Bien sûr la première chose que l'on fait dans la boucle est d'incrémenter le compteur Tir. On continue jusqu'à ce que l'on atteigne 999. Pour Tir= 1000 la condition n'est plus vraie et le bloc d'instructions du while n'est pas exécuté. On passe aux instructions suivantes pour afficher le résultat.
- À chaque tir on teste si on est dans la portion de disque ou pas à l'aide de l'inégalité $x^2+y^2 \leqslant 1$.
- Cette méthode n'est pas très efficace, il faut beaucoup de tirs pour obtenir le deux premières décimales de π.

1.4. Un peu plus sur Python

- Le plus surprenant avec Python c'est que c'est ***l'indentation*** qui détermine le début et la fin d'un bloc d'instructions. Cela oblige à présenter très soigneusement le code.
- Contrairement à d'autres langages on n'a pas besoin de déclarer le type de variable. Par exemple lorsque l'on initialise une variable par x=0, on n'a pas besoin de préciser si x est un entier ou un réel.
- Nous travaillerons avec la version 3 (ou plus) de Python, que l'on appelle par python ou python3. Pour savoir si vous avez la bonne version tester la commande 4/3. Si la réponse est 1.3333... alors tout est ok. Par contre avec les versions 1 et 2 de Python la réponse est 1 (car il considérait que c'est quotient de la division euclidienne de deux entiers).
- La première façon de lancer Python est en ligne de commande, on obtient alors l'invite >>> et on tape les commandes.
- Mais le plus pratique est de sauvegarder ses commandes dans un fichier et de faire un appel par python monfichier.py
- Vous trouverez sans problème de l'aide et des tutoriels sur internet !

Mini-exercices

1. Soit le produit $P_n = (1-\frac{1}{2}) \times (1-\frac{1}{3}) \times (1-\frac{1}{4}) \times \cdots \times (1-\frac{1}{n})$. Calculer une valeur approchée de P_n pour les premiers entiers n.
2. Que vaut la somme des entiers i qui apparaissent dans l'instruction for␣i␣in␣range(1,10). Idem pour for␣i␣in␣range(11). Idem pour for␣i␣in␣range(1,10,2). Idem pour for␣i␣in␣range(0,10,2). Idem pour for␣i␣in␣range(10,0,-1).
3. On considère le cube $[0,1]\times[0,1]\times[0,1]$ et la portion de boule de rayon 1 centrée à l'origine incluse dans ce cube. Faire les calculs de probabilité pour un point tiré au hasard dans le cube d'être en fait dans la portion de boule. Faire une fonction pour le vérifier expérimentalement.
4. On lance deux dés. Expérimenter quelle est la probabilité que la somme soit 7, puis 6, puis 3 ? Quelle est la probabilité que l'un des deux dés soit un 6 ? d'avoir un double ? La fonction randint(a,␣b) du module random retourne un entier k au hasard, vérifiant $a \leqslant k \leqslant b$.
5. On lance un dé jusqu'à ce que l'on obtienne un 6. En moyenne au bout de combien de lancer s'arrête-t-on ?

2. Écriture des entiers

Nous allons faire un peu d'arithmétique : le quotient de la division euclidienne `//`, le reste `%` (modulo) et nous verrons l'écriture des entiers en base 10 et en base 2. Nous utiliserons aussi la notion de listes et le module `math`.

2.1. Division euclidienne et reste, calcul avec les modulo

La division euclidienne de a par b, avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$ s'écrit :

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b$$

où $q \in \mathbb{Z}$ est le ***quotient*** et $r \in \mathbb{N}$ est le ***reste***.
En `Python` le quotient se calcule par : `a // b`. Le reste se calcule par `a % b`. Exemple : `14 // 3` retourne 4 alors que `14 % 3` (lire 14 modulo 3) retourne 2. On a bien $14 = 3 \times 4 + 2$.
Les calculs avec les modulos sont très pratiques. Par exemple si l'on souhaite tester si un entier est pair, ou impair cela revient à un test modulo 2. Le code est `if (n%2 == 0) : ... else : ...`.
Si on besoin de calculer $\cos(n\frac{\pi}{2})$ alors il faut discuter suivant les valeurs de `n%4`.

Appliquons ceci au problème suivant :

Travaux pratiques 4

Combien y-a-t-il d'occurrences du chiffre 1 dans les nombres de 1 à 999 ? Par exemple le chiffre 1 apparaît une fois dans 51 mais deux fois dans 131.

Algorithme . nb-un.py

```
NbDeUn = 0
for N in range(1,999+1) :
    ChiffreUnite = N % 10
    ChiffreDizaine = (N // 10) % 10
    ChiffreCentaine = (N // 100) % 10
    if (ChiffreUnite == 1) :
        NbDeUn = NbDeUn + 1
    if (ChiffreDizaine == 1) :
        NbDeUn = NbDeUn + 1
    if (ChiffreCentaine == 1) :
        NbDeUn = NbDeUn + 1
print("Nombre␣d'occurences␣du␣chiffre␣'1'␣ :", NbDeUn)
```

Commentaires :

- Comment obtient-on le chiffre des unités d'un entier N ? C'est le reste modulo 10, d'où l'instruction `ChiffreUnite = N % 10`.
- Comment obtient-on le chiffre des dizaines ? C'est plus délicat, on commence par effectuer la division euclidienne de N par 10 (cela revient à supprimer le chiffre des unités, par exemple si $N = 251$ alors `N // 10` retourne 25). Il ne reste plus qu'à calculer le reste modulo 10, (par exemple `(N // 10) % 10` retourne le chiffre des dizaines 5.
- Pour le chiffre des centaines on divise d'abord par 100.

2.2. Écriture des nombres en base 10

L'écriture décimale d'un nombre, c'est associer à un entier N la suite de ses chiffres $[a_0, a_1, \ldots, a_n]$ de sorte que a_i soit le i-ème chiffre de N. C'est-à-dire

$$N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0 \quad \text{et } a_i \in \{0, 1, \ldots, 9\}$$

a_0 est le chiffre des unités, a_1 celui des dizaines, a_2 celui des centaines,...

Travaux pratiques 5

1. Écrire une fonction qui à partir d'une liste $[a_0, a_1, \ldots, a_n]$ calcule l'entier N correspondant.
2. Pour un entier N fixé, combien a-t-il de chiffres ? On pourra s'aider d'une inégalité du type $10^n \leqslant N < 10^{n+1}$.
3. Écrire une fonction qui à partir de N calcule son écriture décimale $[a_0, a_1, \ldots, a_n]$.

Voici le premier algorithme :

Algorithme . decimale.py (1)

```
def chiffres_vers_entier(tab) :
    N = 0
    for i in range(len(tab)) :
        N = N + tab[i] * (10 ** i)
    return N
```

La formule mathématique est simplement $N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0$. Par exemple `chiffres_vers_entier([4,3,2,1])` renvoie l'entier 1234.

Expliquons les bases sur les ***listes*** (qui s'appelle aussi des ***tableaux***)

- En `Python` une liste est présentée entre des crochets. Par exemple pour `tab = [4,3,2,1]` alors on accède aux valeurs par `tab[i]` : `tab[0]` vaut 4, `tab[1]` vaut 3, `tab[2]` vaut 2, `tab[3]` vaut 1.
- Pour parcourir les éléments d'un tableau le code est simplement `for x in tab`, x vaut alors successivement 4, 3, 2, 1.
- La longueur du tableau s'obtient par `len(tab)`. Pour notre exemple `len([4,3,2,1])` vaut 4. Pour parcourir toutes les valeurs d'un tableau on peut donc aussi écrire `for i in range(len(tab))`, puis utiliser `tab[i]`, ici i variant ici de 0 à 3.
- La liste vide est seulement notée avec deux crochets : `[]`. Elle est utile pour initialiser une liste.
- Pour ajouter un élément à une liste `tab` existante on utilise la fonction `append`. Par exemple définissons la liste vide `tab=[]`, pour ajouter une valeur à la fin de la liste on saisit : `tab.append(4)`. Maintenant notre liste est [4], elle contient un seul élément. Si on continue avec `tab.append(3)`. Alors maintenant notre liste a deux éléments : [4,3].

Voici l'écriture d'un entier en base 10 :

Algorithme . decimale.py (2)

```
def entier_vers_chiffres(N) :
    tab = []
    n = floor(log(N,10))   # le nombre de chiffres est n+1
    for i in range(0,n+1) :
        tab.append((N // 10 ** i) % 10)
    return tab
```

Par exemple `entier_vers_chiffres(1234)` renvoie le tableau [4,3,2,1]. Nous avons expliqué tout ce dont nous avions besoin sur les listes au-dessus, expliquons les mathématiques.

- Décomposons $\mathbb{N}^*$ sous la forme $[1,10[\, \cup\, [10,100[\, \cup\, [100,1000[\, \cup\, [1000,10000[\, \cup \cdots$ Chaque intervalle est du type $[10^n, 10^{n+1}[$. Pour $N \in \mathbb{N}^*$ il existe donc $n \in \mathbb{N}$ tel que $10^n \leqslant N < 10^{n+1}$. Ce qui indique que le nombre de chiffres de N est $n+1$.
  Par exemple si $N = 1234$ alors $1000 = 10^3 \leqslant N < 10^4 = 10000$, ainsi $n = 3$ et le nombre de chiffres est 4.
- Comment calculer n à partir de N ? Nous allons utiliser le logarithme décimal $\log_{10}$ qui vérifie $\log_{10}(10) = 1$ et $\log_{10}(10^i) = i$. Le logarithme est une fonction croissante, donc l'inégalité $10^n \leqslant N < 10^{n+1}$ devient $\log_{10}(10^n) \leqslant \log_{10}(N) < \log_{10}(10^{n+1})$. Et donc $n \leqslant \log_{10}(N) < n+1$. Ce qui indique donc que $n = E(\log_{10}(N))$ où $E(x)$ désigne la partie entière d'un réel x.

2.3. Module `math`

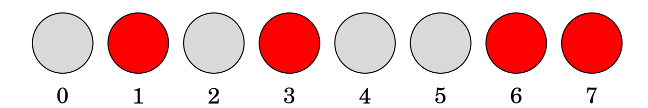
Quelques commentaires informatiques sur un module important pour nous. Les fonctions mathématiques ne sont pas définies par défaut dans `Python` (à part $|x|$ et x^n), il faut faire appel à une librairie spéciale : le module `math` contient les fonctions mathématiques principales.

`abs(x)`	$\|x\|$
`x ** n`	x^n
`sqrt(x)`	$\sqrt{x}$
`exp(x)`	$\exp x$
`log(x)`	$\ln x$ logarithme népérien
`log(x,10)`	$\log x$ logarithme décimal
`cos(x), sin(x), tan(x)`	$\cos x$, $\sin x$, $\tan x$ en radians
`acos(x), asin(x), atan(x)`	$\arccos x$, $\arcsin x$, $\arctan x$ en radians
`floor(x)`	partie entière $E(x)$:plus grand entier $n \leqslant x$ (*floor* = plancher)
`ceil(x)`	plus petit entier $n \geqslant x$ (*ceil* = plafond)

- Comme on aura souvent besoin de ce module on l'appelle par le code `from math import *`. Cela signifie que l'on importe toutes les fonctions de ce module et qu'en plus on n'a pas besoin de préciser que la fonction vient du module `math`. On peut écrire `cos(3.14)` au lieu `math.cos(3.14)`.
- Dans l'algorithme précédent nous avions utilisé le logarithme décimal `log(x,10)`, ainsi que la partie entière `floor(x)`.

2.4. Écriture des nombres en base 2

On dispose d'une rampe de lumière, chacune des 8 lampes pouvant être allumée (rouge) ou éteinte (gris).



On numérote les lampes de 0 à 7. On souhaite contrôler cette rampe : afficher toutes les combinaisons possibles, faire défiler une combinaison de la gauche à droite (la "chenille"), inverser l'état de toutes les lampes,... Voyons comment l'écriture binaire des nombres peut nous aider. L'***écriture binaire*** d'un nombre c'est son écriture en base 2.

Comment calculer un nombre qui est écrit en binaire ? Le chiffre des "dizaines" correspond à 2 (au lieu de 10), le chiffre des "centaines" à $4 = 2^2$ (au lieu de $100 = 10^2$), le chiffres des "milliers" à $8 = 2^3$ (au lieu de $1000 = 10^3$),... Pour le chiffre des unités cela correspond à $2^0 = 1$ (de même que $10^0 = 1$).

Par exemple 10011_b vaut le nombre 19. Car

$$10011_b = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 16 + 2 + 1 = 19.$$

De façon générale tout entier $N \in \mathbb{N}$ s'écrit de manière unique sous la forme

$$N = a_n 2^n + a_{n-1} 2^{n-1} + \cdots + a_2 2^2 + a_1 2 + a_0 \quad \text{et} \quad a_i \in \{0,1\}$$

On note alors $N = a_n a_{n-1} \ldots a_1 a_0\ _b$ (avec un indice b pour indiquer que c'est son écriture binaire).

Travaux pratiques 6

1. Écrire une fonction qui à partir d'une liste $[a_0, a_1, \ldots, a_n]$ calcule l'entier N correspondant à l'écriture binaire $a_n a_{n-1} \ldots a_1 a_0\ _b$.
2. Écrire une fonction qui à partir de N calcule son écriture binaire sous la forme $[a_0, a_1, \ldots, a_n]$.

La seule différence avec la base 10 c'est que l'on calcule avec des puissances de 2.

Algorithme . binaire.py (1)

```
def binaire_vers_entier(tab) :
    N = 0
    for i in range(len(tab)) :
        N = N + tab[i] * (2 ** i)
    return N
```

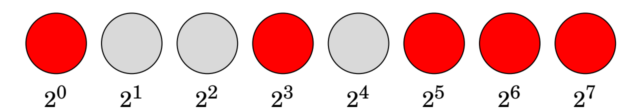
Idem pour le sens inverse où l'on a besoin du logarithme en base 2, qui vérifie $\log_2(2) = 1$ et $\log_2(2^i) = i$.

Algorithme . binaire.py (2)

```
def entier_vers_binaire(N) :
    tab = []
    n = floor(log(N,2))   # le nombre de chiffres est n+1
```

```
    for i in range(0,n+1) :
        tab.append((N // 2 ** i) % 2)
    return tab
```

Maintenant appliquons ceci à notre problème de lampes. Si une lampe est allumée on lui attribut 1, et si elle est éteinte 0. Pour une rampe de 8 lampes on code $[a_0, a_1, \dots, a_7]$ l'état des lampes. Par exemple la configuration suivante :



est codé $[1,0,0,1,0,1,1,1]$ ce qui correspond au nombre binaire $11101001_b = 233$.

Travaux pratiques 7

1. Faire une boucle qui affiche toutes les combinaisons possibles (pour une taille de rampe donnée).
2. Quelle opération mathématique élémentaire transforme un nombre binaire $a_n \dots a_1 a_0\ _b$ en $a_n \dots a_1 a_0 0\ _b$ (décalage vers la gauche et ajout d'un 0 à la fin) ?
3. Soit $N' = a_n a_{n-1} \dots a_1 a_0 0\ _b$ (une écriture avec $n+2$ chiffres). Quelle est l'écriture binaire de $N' \pmod{2^{n+1}}$? (C'est une écriture avec $n+1$ chiffres.)
4. En déduire un algorithme qui pour une configuration donnée de la rampe, fait permuter cycliquement (vers la droite) cette configuration. Par exemple $[1,0,1,0,1,1,1,0]$ devient $[0,1,0,1,0,1,1,1]$.
5. Quelle opération mathématique élémentaire permet de passer d'une configuration à son opposée (une lampe éteinte s'allume, et réciproquement). Par exemple si la configuration était $[1,0,1,0,1,1,1,0]$ alors on veut $[0,1,0,1,0,0,0,1]$. (Indication : sur cet exemple calculer les deux nombres correspondants et trouver la relation qui les lie.)

1. Il s'agit d'abord d'afficher les configurations. Par exemple si l'on a 4 lampes alors les configurations sont $[0,0,0,0]$, $[1,0,0,0]$, $[0,1,0,0]$, $[1,1,0,0]$,..., $[1,1,1,1]$. Pour chaque lampe nous avons deux choix (allumé ou éteint), il y a $n+1$ lampes donc un total de 2^{n+1} configurations. Si l'on considère ces configurations comme des nombres écrits en binaire alors l'énumération ci-dessus correspond à compter $0,1,2,3,\dots,2^{n+1}-1$.
   D'où l'algorithme :

   Algorithme . binaire.py (3)

   ```
   def configurations(n) :
       for N in range(2**(n+1)) :
           print(entier_vers_binaire_bis(N,n))
   ```

   Où `entier_vers_binaire_bis(N,n)` est similaire à `entier_vers_binaire(N)`, mais en affichant aussi les zéros non significatifs, par exemple 7 en binaire s'écrit 111_b, mais codé sur 8 chiffres on ajoute devant des 0 non significatifs : 00000111_b.
2. En écriture décimale, multiplier par 10 revient à décaler le nombre initial et rajouter un zéro. Par exemple $10 \times 19 = 190$. C'est la même chose en binaire ! Multiplier un nombre par 2

revient sur l'écriture à un décalage vers la gauche et ajout d'un zéro sur le chiffre des unités. Exemple : $19 = 10011_b$ et $2 \times 19 = 38$ donc $2 \times 10011_b = 100110_b$.

3. Partant de $N = a_n a_{n-1} \dots a_1 a_0 \ _b$. Notons $N' = 2N$, son écriture est $N' = a_n a_{n-1} \dots a_1 a_0 0 \ _b$. Alors $N' \pmod{2^{n+1}}$ s'écrit exactement $a_{n-1} a_{n-2} \dots a_1 a_0 0 \ _b$ et on ajoute a_n qui est le quotient de N' par 2^{n+1}.

   Preuve : $N' = a_n \cdot 2^{n+1} + a_{n-1} \cdot 2^n + \cdots + a_0 \cdot 2$. Donc $N' \pmod{2^{n+1}} = a_{n-1} \cdot 2^n + \cdots + a_0 \cdot 2$. Donc $N' \pmod{2^{n+1}} + a_n = a_{n-1} \cdot 2^n + \cdots + a_0 \cdot 2 + a_n$.

4. Ainsi l'écriture en binaire de $N' \pmod{2^{n+1}} + a_n$ s'obtient comme permutation circulaire de celle de N. D'où l'algorithme :

   Algorithme . binaire.py (4)

```
def decalage(tab) :
    N = binaire_vers_entier(tab)
    n = len(tab)-1   # le nombre de chiffres est n+1
    NN = 2*N % 2**(n+1) + 2*N // 2**(n+1)
    return entier_vers_binaire_bis(NN,n)
```

5. On remarque que si l'on a deux configurations opposées alors leur somme vaut $2^{n+1} - 1$: par exemple avec $[1,0,0,1,0,1,1,1]$ et $[0,1,1,0,1,0,0,0]$, les deux nombres associés sont $N = 11101001_b$ et $N' = 00010110_b$ (il s'agit juste de les réécrire de droite à gauche). La somme est $N + N' = 11101001_b + 00010110_b = 11111111_b = 2^8 - 1$. L'addition en écriture binaire se fait de la même façon qu'en écriture décimale et ici il n'y a pas de retenue. Si M est un nombre avec $n+1$ fois le chiffres 1 alors $M + 1 = 2^{n+1}$. Exemple si $M = 11111_b$ alors $M + 1 = 100000_b = 2^5$; ainsi $M = 2^5 - 1$. Donc l'opposé de N est $N' = 2^{n+1} - 1 - N$ (remarquez que dans $\mathbb{Z}/(2^{n+1} - 1)\mathbb{Z}$ alors $N' \equiv -N$).

   Cela conduit à :

   Algorithme . binaire.py (5)

```
def inversion(tab) :
    N = binaire_vers_entier(tab)
    n = len(tab)-1   # le nombre de chiffres est n+1
    NN = 2**(n+1)-1 - N
    return entier_vers_binaire_bis(NN,n)
```

Mini-exercices

1. Pour un entier n fixé, combien y-a-t-il d'occurrences du chiffre 1 dans l'écriture des nombres de 1 à n ?
2. Écrire une fonction qui calcule l'écriture décimale d'un entier, sans recourir au log (une boucle `while` est la bienvenue).
3. Écrire un algorithme qui permute cycliquement une configuration de rampe vers la droite.
4. On dispose de $n+1$ lampes, chaque lampe peut s'éclairer de trois couleurs : vert, orange,

rouge (dans cet ordre). Trouver toutes les combinaisons possibles. Comment passer toutes les lampes à la couleur suivante ?

5. Générer toutes les matrices 4×4 n'ayant que des 0 et des 1 comme coefficients. On codera une matrice sous la forme de lignes [[1,1,0,1],[0,0,1,0],[1,1,1,1],[0,1,0,1]].
6. On part du point $(0,0) \in \mathbb{Z}^2$. A chaque pas on choisit au hasard un direction Nord, Sud, Est, Ouest. Si on va au Nord alors on ajoute $(0,1)$ à sa position (pour Sud on ajoute $(0,-1)$; pour Est $(1,0)$; pour Ouest $(-1,0)$). Pour un chemin d'une longueur fixée de n pas, coder tous les chemins possibles. Caractériser les chemins qui repassent par l'origine. Calculer la probabilité p_n de repasser par l'origine. Que se passe-t-il lorsque $n \to +\infty$?
7. Écrire une fonction, qui pour un entier N, affiche son écriture en chiffres romains : $M = 1000$, $D = 500$, $C = 100$, $X = 10$, $V = 5$, $I = 1$. Il ne peut y avoir plus de trois symboles identiques à suivre.

3. Calculs de sinus, cosinus, tangente

Le but de cette section est le calcul des sinus, cosinus, et tangente d'un angle par nous même, avec une précision de 8 chiffres après la virgule.

3.1. Calcul de $\operatorname{Arctan} x$

Nous aurons besoin de calculer une fois pour toute $\operatorname{Arctan}(10^{-i})$, pour $i = 0, \ldots, 8$, c'est-à-dire que l'on cherche les angles $\theta_i \in]-\frac{\pi}{2}, \frac{\pi}{2}[$ tels que $\tan \theta_i = 10^{-i}$. Nous allons utiliser la formule :

$$\operatorname{Arctan} x = \sum_{k=0}^{+\infty} (-1)^k \frac{x^{2k+1}}{2k+1} = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots$$

Travaux pratiques 8

1. Calculer $\operatorname{Arctan} 1$.
2. Calculer $\theta_i = \operatorname{Arctan} 10^{-i}$ (avec 8 chiffres après la virgule) pour $i = 1, \ldots, 8$.
3. Pour quelles valeurs de i, l'approximation $\operatorname{Arctan} x \simeq x$ était-elle suffisante ?

Algorithme . tangente.py (1)

```
def mon_arctan(x,n) :
    somme = 0
    for k in range(0,n+1) :
        if (k%2 == 0) :  # si k est pair signe +
            somme = somme + 1/(2*k+1) * (x ** (2*k+1))
        else :           # si k est impair signe -
            somme = somme - 1/(2*k+1) * (x ** (2*k+1))
    return somme
```

– La série qui permet de calculer $\operatorname{Arctan} x$ est une somme infinie, mais si x est petit alors chacun des termes $(-1)^k \frac{x^{2k+1}}{2k+1}$ est très très petit dès que k devient grand. Par exemple si

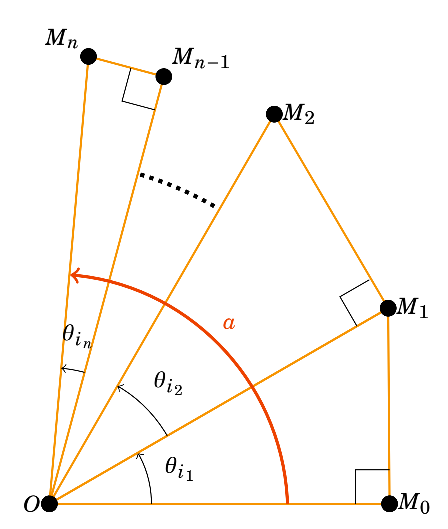
$0 \leqslant x \leqslant \frac{1}{10}$ alors $x^{2k+1} \leqslant \frac{1}{10^{2k+1}}$ et donc pour $k \geqslant 4$ nous aurons $\left|(-1)^k \frac{x^{2k+1}}{2k+1}\right| < 10^{-9}$. Chacun des termes suivants ne contribue pas aux 8 premiers chiffres après la virgule. Attention : il se pourrait cependant que la somme de beaucoup de termes finissent par y contribuer, mais ce n'est pas le cas ici (c'est un bon exercice de le prouver).

- Dans la pratique on calcule la somme à un certain ordre $2k+1$ jusqu'à ce que les 8 chiffres après la virgules ne bougent plus. Et en fait on s'aperçoit que l'on a seulement besoin d'utiliser $\operatorname{Arctan} x \simeq x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7}$.
- Pour $i \geqslant 4$, $\operatorname{Arctan} x \simeq x$ donne déjà 8 chiffres exacts après la virgule !

On remplit les valeurs des angles θ_i obtenus dans une liste nommée `theta`.

3.2. Calcul de $\tan x$

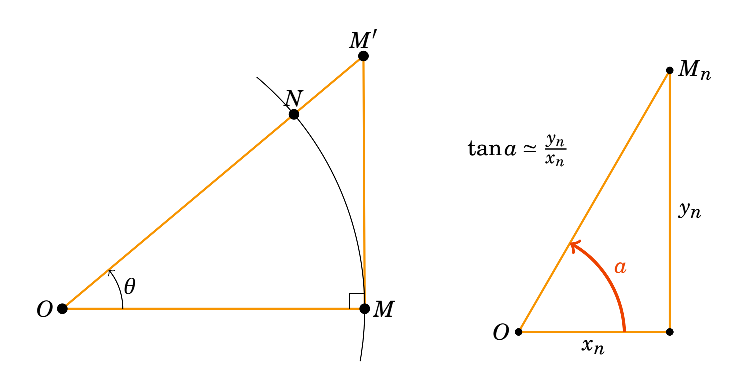
Le principe est le suivant : on connaît un certain nombre d'angles avec leur tangente : les angles θ_i (calculés ci-dessus) avec par définition $\tan \theta_i = 10^{-i}$. Fixons un angle $a \in [0, \frac{\pi}{2}]$. Partant du point $M_0 = (1,0)$, nous allons construire des points $M_1, M_2, \ldots, M_n$ jusqu'à ce que M_n soit (à peu près) sur la demi-droite correspondant à l'angle a. Si M_n a pour coordonnées (x_n, y_n) alors $\tan a = \frac{y_n}{x_n}$. L'angle pour passer d'un point M_k à M_{k+1} est l'un des angles θ_i.



Rappelons que si l'on a un point $M(x,y)$ alors la rotation centrée à l'origine et d'angle θ envoie $M(x,y)$ sur le point $N(x',y')$ avec

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{c'est-à-dire} \quad \begin{cases} x' = x\cos\theta - y\sin\theta \\ y' = x\sin\theta + y\cos\theta \end{cases}$$

Pour un point M, on note M' le point de la demi-droite $[ON)$ tel que les droites (OM) et (MM') soient perpendiculaires en M.



Travaux pratiques 9

1(a) Calculer la longueur OM'.

(b) En déduire les coordonnées de M'.

(c) Exprimez-les uniquement en fonction de x, y et $\tan\theta$.

2. Faire une boucle qui décompose l'angle a en somme d'angles θ_i (à une précision de 10^{-8} ; avec un minimum d'angles, les angles pouvant se répéter).

3. Partant de $M_0 = (1,0)$ calculer les coordonnées des différents M_k, jusqu'au point $M_n(x_n, y_n)$ correspondant à l'approximation de l'angle a. Renvoyer la valeur $\frac{y_n}{x_n}$ comme approximation de $\tan a$.

Voici les préliminaires mathématiques :

- Dans le triangle rectangle OMM' on a $\cos\theta = \frac{OM}{OM'}$ donc $OM' = \frac{OM}{\cos\theta}$.
- D'autre part comme la rotation d'angle θ conserve les distances alors $OM = ON$. Si les coordonnées de M' sont (x'', y'') alors $x'' = \frac{1}{\cos\theta}x'$ et $y'' = \frac{1}{\cos\theta}y'$.
- Ainsi
$$\begin{cases} x'' = \frac{1}{\cos\theta}x' = \frac{1}{\cos\theta}\big(x\cos\theta - y\sin\theta\big) = x - y\tan\theta \\ y'' = \frac{1}{\cos\theta}y' = \frac{1}{\cos\theta}\big(x\sin\theta + y\cos\theta\big) = x\tan\theta + y \end{cases}$$
Autrement dit :
$$\begin{pmatrix} x'' \\ y'' \end{pmatrix} = \begin{pmatrix} 1 & -\tan\theta \\ \tan\theta & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Voici une boucle simple pour décomposer l'angle θ : on commence par retirer le plus grand angle θ_0 autant de fois que l'on peut, lorsque ce n'est plus possible on passe à l'angle θ_1,...

Algorithme . tangente.py (2)

```
i = 0
while (a > precision) :     # boucle tant que la precision pas atteinte
    while (a < theta[i]) :  # choix du bon angle theta_i à soustraire
        i = i+1
    a = a - theta[i]       # on retire l'angle theta_i et on recommence
```

Ici `precision` est la précision souhaité (pour nous 10^{-9}). Et le tableau `theta` contient les valeurs des angles θ_i.

Posons $x_0 = 1$, $y_0 = 0$ et $M_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$. Alors on définit par récurrence $M_{k+1} = P(\theta_i) \cdot M_k$ où $P(\theta) = \begin{pmatrix} 1 & -\tan\theta \\ \tan\theta & 1 \end{pmatrix}$. Les θ_i sont ceux apparaissant dans la décomposition de l'angle en somme de θ_i, donc on connaît $\tan\theta_i = 10^{-i}$. Ainsi si l'on passe d'un point M_k à M_{k+1} par un angle θ_i on a simplement :
$$\begin{cases} x_{k+1} = x_k - y_k \cdot 10^{-i} \\ y_{k+1} = x_k \cdot 10^{-i} + y_k \end{cases}$$

La valeur $\frac{y_n}{x_n}$ est la tangente de la somme des angles θ_i, donc une approximation de $\tan a$.
Le code est maintenant le suivant.

Algorithme . tangente.py (3)

```
def ma_tan(a) :
    precision = 10**(-9)
    i = 0  ; x = 1  ; y = 0
    while (a > precision) :
        while (a < theta[i]) :
            i = i+1
        newa = a - theta[i]       # on retire l'angle theta_i
        newx = x - (10**(-i))*y   # on calcule le nouveau point
        newy = (10**(-i))*x + y
        x = newx
        y = newy
        a = newa
    return y/x                    # on renvoie la tangente
```

Commentaires pour conclure :

- En théorie il ne faut pas confondre «précision» et «nombre de chiffres exacts après la virgule». Par exemple 0.999 est une valeur approchée de 1 à 10^{-3} près, mais aucun chiffre après la virgule n'est exact. Dans la pratique c'est la précision qui importe plus que le nombre de chiffres exacts.
- Notez à quel point les opérations du calcul de $\tan x$ sont simples : il n'y a quasiment que des additions à effectuer. Par exemple l'opération $x_{k+1} = x_k - y_k \cdot 10^{-i}$ peut être fait à la main : multiplier par 10^{-i} c'est juste décaler la virgule à droite de i chiffres, puis on additionne. C'est cet algorithme «CORDIC» qui est implémenté dans les calculatrices, car il nécessite très peu de ressources. Bien sûr, si les nombres sont codés en binaire on remplace les 10^{-i} par 2^{-i} pour n'avoir qu'à faire des décalages à droite.

3.3. Calcul de $\sin x$ et $\cos x$

Travaux pratiques 10

Pour $0 \leqslant x \leqslant \frac{\pi}{2}$, calculer $\sin x$ et $\cos x$ en fonction de $\tan x$. En déduire comment calculer les sinus et cosinus de x.

Solution : On sait $\cos^2 + \sin^2 x = 1$, donc en divisant par $\cos^2 x$ on trouve $1 + \tan^2 x = \frac{1}{\cos^2 x}$. On en déduit que pour $0 \leqslant x \leqslant \frac{\pi}{2}$ $\cos x = \frac{1}{\sqrt{1+\tan^2 x}}$. On trouve de même $\sin x = \frac{\tan x}{\sqrt{1+\tan^2 x}}$.
Donc une fois que l'on a calculé $\tan x$ on en déduit $\sin x$ et $\cos x$ par un calcul de racine carrée. Attention c'est valide car x est compris entre 0 et $\frac{\pi}{2}$. Pour un x quelconque il faut se ramener par les formules trigonométriques à l'intervalle $[0, \frac{\pi}{2}]$.

Mini-exercices

1. On dispose de billets de 1, 5, 20 et 100 euros. Trouvez la façon de payer une somme de n euros avec le minimum de billets.
2. Faire un programme qui pour **n'importe quel** $x \in \mathbb{R}$, calcule $\sin x$, $\cos x$, $\tan x$.

3. Pour $t = \tan\frac{x}{2}$ montrer que $\tan x = \frac{2t}{1-t^2}$. En déduire une fonction qui calcule $\tan x$. (Utiliser que pour x assez petit $\tan x \simeq x$).
4. Modifier l'algorithme de la tangente pour qu'il calcule aussi directement le sinus et le cosinus.

4. Les réels

Dans cette partie nous allons voir différentes façons de calculer la constante γ d'Euler. C'est un nombre assez mystérieux car personne ne sait si γ est un nombre rationnel ou irrationnel. Notre objectif est d'avoir le plus de décimales possibles après la virgule en un minimum d'étapes. Nous verrons ensuite comment les ordinateurs stockent les réels et les problèmes que cela engendre.

4.1. Constante γ d'Euler

Considérons la ***suite harmonique*** :

$$H_n = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

et définissons

$$u_n = H_n - \ln n.$$

Cette suite (u_n) admet une limite lorsque $n \to +\infty$: c'est la ***constante γ d'Euler***.

Travaux pratiques 11

1. Calculer les premières décimales de γ. Sachant que $u_n - \gamma \sim \frac{1}{2n}$, combien de décimales exactes peut-on espérer avoir obtenues ?
2. On considère $v_n = H_n - \ln\left(n + \frac{1}{2} + \frac{1}{24n}\right)$. Sachant $v_n - \gamma \sim -\frac{1}{48n^3}$, calculer davantage de décimales.

Algorithme . euler.py (1)

```
def euler1(n) :
    somme = 0
    for i in range(n,0,-1) :
        somme = somme + 1/i
    return somme - log(n)
```

Algorithme . euler.py (2)

```
def euler2(n) :
    somme = 0
    for i in range(n,0,-1) :
        somme = somme + 1/i
    return somme - log(n+1/2+1/(24*n))
```

Vous remarquez que la somme est calculée à partir de la fin. Nous expliquerons pourquoi en fin de section.

4.2. 1000 décimales de la constante d'Euler

Il y a deux techniques pour obtenir plus de décimales : (i) pousser plus loin les itérations, mais pour avoir 1000 décimales de γ les méthodes précédentes sont insuffisantes ; (ii) trouver une méthode encore plus efficace. C'est ce que nous allons voir avec la méthode de Bessel modifiée. Soit

$$w_n = \frac{A_n}{B_n} - \ln n \quad \text{avec} \quad A_n = \sum_{k=1}^{E(\alpha n)} \left(\frac{n^k}{k!}\right)^2 H_k \quad \text{et} \quad B_n = \sum_{k=0}^{E(\alpha n)} \left(\frac{n^k}{k!}\right)^2$$

où $\alpha = 3.59112147...$ est la solution de $\alpha(\ln \alpha - 1) = 1$ et $E(x)$ désigne la partie entière. Alors

$$|w_n - \gamma| \leqslant \frac{C}{e^{4n}}$$

où C est une constante (non connue).

Travaux pratiques 12

1. Programmer cette méthode.
2. Combien d'itérations faut-il pour obtenir 1000 décimales ?
3. Utiliser le module `decimal` pour les calculer.

Voici le code :

Algorithme . euler.py (3)

```
def euler3(n) :
    alpha = 3.59112147
    N = floor(alpha*n)      # Borne des sommes
    A = 0  ; B = 0
    H = 0
    for k in range(1,N+1) :
        c = ( (n**k)/factorial(k) ) ** 2   # Coefficient commun
        H = H + 1/k                        # Somme harmonique
        A = A + c*H
        B = B + c
    return A/B - log(n)
```

Pour obtenir N décimales il faut résoudre l'inéquation $\frac{C}{e^{4n}} \leqslant \frac{1}{10^N}$. On «passe au log» pour obtenir $n \geqslant \frac{N\ln(10)+\ln(C)}{4}$. On ne connaît pas C mais ce n'est pas si important. Moralement pour une itération de plus on obtient (à peu près) une décimale de plus (c'est-à-dire un facteur 10 sur la précision !). Pour $n \geqslant 800$ on obtient 1000 décimales exactes de la constante d'Euler :

0,

5772156649015328606065120900824024310421593359992
35988057672348848677267776646709369470632917467495
14631447249807082480960504014486542836224173997644
92353625350033374293733773767394279259525824709491
60087352039481656708532331517766115286211995015079
84793745085705740029921354786146694029604325421519
05877553526733139925401296742051375413954911168510
28079842348775872050384310939973613725530608893312

67600172479537836759271351577226102734929139407984
30103417771778088154957066107501016191663340152278
93586796549725203621287922655595366962817638879272
68013243101047650596370394739495763890657296792960
10090151251959509222435014093498712282479497471956
46976318506676129063811051824197444867836380861749
45516989279230187739107294578155431600500218284409
60537724342032854783670151773943987003023703395183
28690001558193988042707411542227819716523011073565
83396734871765049194181230004065469314299929777956
93031005030863034185698032310836916400258929708909
85486825777364288253954925873629596133298574739302

Pour obtenir plus de décimales que la précision standard de `Python`, il faut utiliser le module `decimal` qui permet de travailler avec une précision arbitraire fixée.

4.3. Un peu de réalité

En mathématique un réel est un élément de $\mathbb{R}$ et son écriture décimale est souvent infinie après la virgule : par exemple $\pi = 3,14159265\ldots$ Mais bien sûr un ordinateur ne peut pas coder une infinité d'informations. Ce qui se rapproche d'un réel est un ***nombre flottant*** dont l'écriture est :

$$\underbrace{\pm 1,234567890123456789}_{\text{mantisse}} \; e \; \underbrace{\pm 123}_{\text{exposant}}$$

pour $\pm 1,234\ldots \times 10^{\pm 123}$. La ***mantisse*** est un nombre décimal (positif ou négatif) appartenant à $[1,10[$ et l'exposant est un entier (lui aussi positif ou négatif). En `Python` la mantisse à une précision de 16 chiffres après la virgule.
Cette réalité informatique fait que des erreurs de calculs peuvent apparaître même avec des opérations simples. Pour voir un exemple de problème faites ceci :

Travaux pratiques 13

Poser $x = 10^{-16}$, $y = x+1$, $z = y-1$. Que vaut z pour `Python` ?

Comme `Python` est très précis nous allons faire une routine qui permet de limiter drastiquement le nombre de chiffres et mettre en évidence les erreurs de calculs.

Travaux pratiques 14

1. Calculer l'exposant d'un nombre réel. Calculer la mantisse.
2. Faire une fonction qui ne conserve que 6 chiffres d'un nombre (6 chiffres en tout : avant + après la virgule, exemple 123,456789 devient 123,456).

Voici le code :

Algorithme . reels.py (1)

```
precision = 6                 # Nombre de décimales conservées
def tronquer(x) :
    n = floor(log(x,10))                # Exposant
    m = floor( x * 10 ** (precision-1 - n))  # Mantisse
```

```
    return m * 10 ** (-precision+1+n)        # Nombre tronqué
```

Comme on l'a déjà vu auparavant l'exposant se récupère à l'aide du logarithme en base 10. Et pour tronquer un nombre avec 6 chiffres, on commence par le décaler vers la gauche pour obtenir 6 chiffres avant la virgule ($123,456789$ devient $123456,789$) il ne reste plus qu'à prendre la partie entière (123456) et le redécaler vers la droite (pour obtenir $123,456$).

Absorption

Travaux pratiques 15

1. Calculer `tronquer(1234.56 + 0.007)`.
2. Expliquer.

Chacun des nombres $1234,56$ et $0,007$ est bien un nombre s'écrivant avec moins de 6 décimales mais leur somme $1234,567$ a besoin d'une décimale de plus, l'ordinateur ne retient pas la 7-ème décimale et ainsi le résultat obtenu est $1234,56$. Le $0,007$ n'apparaît pas dans le résultat : il a été victime d'une ***absorption***.

Élimination

Travaux pratiques 16

1. Soient $x = 1234,8777$, $y = 1212,2222$. Calculer $x - y$ à la main. Comment se calcule la différence $x - y$ avec notre précision de 6 chiffres ?
2. Expliquer la différence.

Comme $x - y = 22,6555$ qui n'a que 6 chiffres alors on peut penser que l'ordinateur va obtenir ce résultat. Il n'en est rien, l'ordinateur ne stocke pas x mais `tronquer(x)`, idem pour y. Donc l'ordinateur effectue en fait le calcul suivant : `tronquer(tronquer(x)-tronquer(y))`, il calcule donc $1234,87 - 1212,22 = 22,65$. Quel est le problème ? C'est qu'ensuite l'utilisateur considère –à tort– que le résultat est calculé avec une précision de 6 chiffres. Donc on peut penser que le résultat est $22,6500$ mais les 2 derniers chiffres sont une pure invention.
C'est un phénomène d'***élimination***. Lorsque l'on calcule la différence de deux nombres proches, le résultat a en fait une précision moindre. Cela peut être encore plus dramatique avec l'exemple $\delta = 1234,569 - 1234,55$ la différence est $0,01900$ alors que l'ordinateur retournera $0,01000$. Il y a presque un facteur deux, et on aura des problèmes si l'on a besoin de diviser par δ.

Signalons au passage une erreur d'interprétation fréquente : ne pas confondre la ***précision*** d'affichage (exemple : on calcule avec 10 chiffres après la virgule) avec l'***exactitude*** du résultat (combien de décimales sont vraiment exactes ?).

Conversion binaire – décimale

Enfin le problème le plus troublant est que les nombres flottants sont stockés en écriture binaire et pas en écriture décimale.

Travaux pratiques 17

Effectuer les commandes suivantes et constater !

1. `sum = 0` puis `for i in range(10) : sum = sum + 0.1`. Que vaut `sum` ?
2. `0.1 + 0.1 == 0.2` et `0.1 + 0.1 + 0.1 == 0.3`
3. `x = 0.2 ; print("0.2 en Python = %.25f" %x)`

La raison est simple mais néanmoins troublante. L'ordinateur ne stocke pas $0,1$, ni $0,2$ en mémoire mais le nombre en écriture binaire qui s'en rapproche le plus.
En écriture décimale, il est impossible de coder $1/3 = 0,3333\ldots$ avec un nombre fini de chiffres après la virgule. Il en va de même ici : l'ordinateur ne peut pas stocker exactement $0,2$. Il stocke un nombre en écriture binaire qui s'en rapproche le plus ; lorsqu'on lui demande d'afficher le nombre stocké, il retourne l'écriture décimale qui se rapproche le plus du nombre stocké, mais ce n'est plus $0,2$, mais un nombre très très proche :

`0.2000000000000000111022302...`

4.4. Somme des inverses des carrés

Voyons une situation concrète où ces problèmes apparaissent.

Travaux pratiques 18

1. Faire une fonction qui calcule la somme $S_n = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2}$.
2. Faire une fonction qui calcule cette somme mais en utilisant seulement une écriture décimale à 6 chiffres (à l'aide de la fonction `tronquer()` vue au-dessus).
3. Reprendre cette dernière fonction, mais en commençant la somme par les plus petits termes.
4. Comparez le deux dernières méthodes, justifier et conclure.

La première fonction ne pose aucun problème et utilise toute la précision de `Python`.
Dans la seconde on doit, à chaque calcul, limiter notre précision à 6 chiffres (ici 1 avant la virgule et 5 après).

Algorithme . reels.py (2)

```
def somme_inverse_carres_tronq(n) :
  somme = 0
  for i in range(1,n+1) :
      somme = tronquer(somme + tronquer(1/(i*i)))
  return somme
```

Il est préférable de commencer la somme par la fin :

Algorithme . reels.py (3)

```
def somme_inverse_carres_tronq_inv(n) :
  somme = 0
  for i in range(n,0,-1) :
      somme = tronquer(somme + tronquer(1/(i*i)))
  return somme
```

Par exemple pour $n = 100\,000$ l'algorithme `somme_inverse_carres_tronq()` (avec écriture tronquée, sommé dans l'ordre) retourne $1,64038$ alors que l'algorithme `somme_inverse_carres_tronq_inv()` (avec la somme dans l'ordre inverse) on obtient $1,64490$. Avec une précision maximale et n très grand on doit obtenir $1,64493\ldots$ (en fait c'est $\frac{\pi^2}{6}$).
Notez que faire grandir n pour l'algorithme `somme_inverse_carres_tronq()` n'y changera rien, il bloque à 2 décimales exactes après la virgule : $1,64038$! La raison est un phénomène d'absorption : on rajoute des termes très petits devant une somme qui vaut plus de 1. Alors que si l'on part des termes petits, on ajoute des termes petits à une somme petite, on garde donc un maximum de décimales valides avant de terminer par les plus hautes valeurs.

Mini-exercices

1. Écrire une fonction qui approxime la constante α qui vérifie $\alpha(\ln\alpha - 1) = 1$. Pour cela poser $f(x) = x(\ln x - 1) - 1$ et appliquer la méthode de Newton : fixer u_0 (par exemple ici $u_0 = 4$) et $u_{n+1} = u_n - \frac{f(u_n)}{f'(u_n)}$.
2. Pour chacune des trois méthodes, calculer le nombre approximatif d'itérations nécessaires pour obtenir 100 décimales de la constante γ d'Euler.
3. Notons $C_n = \frac{1}{4n}\sum_{k=0}^{2n} \frac{[(2k)!]^3}{(k!)^4(16n)^{2k}}$. La formule de Brent-McMillan affirme $\gamma = \frac{A_n}{B_n} - \frac{C_n}{B_n^2} - \ln n + O(\frac{1}{e^{8n}})$ où cette fois les sommations pour A_n et B_n vont jusqu'à $E(\beta n)$ avec $\beta = 4,970625759\ldots$ la solution de $\beta(\ln\beta - 1) = 3$. La notation $O(\frac{1}{e^{8n}})$ indique que l'erreur est $\leqslant \frac{C}{e^{8n}}$ pour une certaine constante C. Mettre en œuvre cette formule. En 1999 cette formule a permis de calculer 100 millions de décimales. Combien a-t-il fallu d'itérations ?
4. Faire une fonction qui renvoie le terme u_n de la suite définie par $u_0 = \frac{1}{3}$ et $u_{n+1} = 4u_n - 1$. Que vaut u_{100} ? Faire l'étude mathématique et commenter.

5. Arithmétique – Algorithmes récursifs

Nous allons présenter quelques algorithmes élémentaires en lien avec l'arithmétique. Nous en profitons pour présenter une façon complètement différente d'écrire des algorithmes : les fonctions récursives.

5.1. Algorithmes récursifs

Voici un algorithme très classique :

Algorithme . recursif.py (1)

```
def factorielle_classique(n) :
    produit = 1
    for i in range(1,n+1) :
        produit = i * produit
    return produit
```

Voyons comment fonctionne cette boucle. On initialise la variable `produit` à 1, on fait varier un indice i de 1 à n. À chaque étape on multiplie `produit` par i et on affecte le résultat dans `produit`. Par exemple si $n = 5$ alors la variable `produit` s'initialise à 1, puis lorsque i varie la variable produit devient $1 \times 1 = 1$, $2 \times 1 = 2$, $3 \times 2 = 6$, $4 \times 6 = 24$, $5 \times 24 = 120$. Vous avez bien sûr reconnus le calcul de 5!

Étudions un autre algorithme.

Algorithme . recursif.py (2)

```
def factorielle(n) :
    if (n==1) :
        return 1
    else :
        return n * factorielle(n-1)
```

Que fait cet algorithme ? Voyons cela pour $n = 5$. Pour $n = 5$ la condition du «si» (if) n'est pas vérifiée donc on passe directement au «sinon» (else). Donc `factorielle(5)` renvoie comme résultat : `5 * factorielle(4)`. On a plus ou moins progressé : le calcul n'est pas fini car on ne connaît pas encore `factorielle(4)` mais on s'est ramené à un calcul au rang précédent, et on itère : `factorielle(5) = 5 * factorielle(4) = 5 * 4 * factorielle(3) = 5 * 4 * 3 * factorielle(2)` et enfin `factorielle(5) = 5 * 4 * 3 * 2 * factorielle(1)`. Pour `factorielle(1)` la condition du `if (n==1)` est vérifiée et alors `factorielle(1)=1`. Le bilan est donc que `factorielle(5) = 5 * 4 * 3 *` c'est bien 5!

Une fonction qui lorsque elle s'exécute s'appelle elle-même est une ***fonction récursive***. Il y a une analogie très forte avec la récurrence. Par exemple on peut définir la suite des factorielles ainsi :

$$u_1 = 1 \quad \text{et} \quad u_n = n \times u_{n-1} \text{ si } n \geqslant 2.$$

Nous avons ici $u_n = n!$ pour tout $n \geqslant 1$.

Comme pour la récurrence une fonction récursive comporte une étape d'***initialisation*** (ici `if (n==1) : return 1` correspondant à $u_1 = 1$) et une étape d'***hérédité*** (ici `return n * factorielle(n-1)` correspondant à $u_n = n \times u_{n-1}$).

On peut même faire deux appels à la fonction :

Algorithme . recursif.py (3)

```
def fibonacci(n) :
    if (n==0) or (n==1) :
        return 1
    else :
        return fibonacci(n-1)+fibonacci(n-2)
```

Faites-le calcul de `fibonacci(5)`. Voici la version mathématique des nombres de Fibonacci.

$$F_0 = 1,\ F_1 = 1 \quad \text{et} \quad F_n = F_{n-1} + F_{n-2} \quad \text{si } n \geqslant 2.$$

On obtient un nombre en additionnant les deux nombres des rangs précédents :

$$1 \quad 1 \quad 2 \quad 3 \quad 5 \quad 8 \quad 13 \quad 21 \quad 34 \quad \ldots$$

5.2. L'algorithme d'Euclide

L'algorithme d'Euclide est basé sur le principe suivant

$$\text{si } b|a \text{ alors } \operatorname{pgcd}(a,b) = b \qquad \text{sinon } \operatorname{pgcd}(a,b) = \operatorname{pgcd}(b, a \bmod b)$$

Travaux pratiques 19

1. Créer une fonction récursive `pgcd(a,b)` qui calcule le pgcd.
2. On note p_n la probabilité que deux entiers a,b tirés au hasard dans $1,2,\ldots,n$ soient premiers entre eux. Faire une fonction qui approxime p_n. Lorsque n devient grand, comparer p_n et $\frac{6}{\pi^2}$.

Voici le code pour l'algorithme d'Euclide récursif. Notez à quel point le code est succinct et épuré !

Algorithme . arith.py (1)

```
def pgcd(a,b) :
    if a%b == 0 :
        return b
    else :
        return pgcd(b, a%b)
```

Deux entiers a,b sont premiers entre eux ssi $\operatorname{pgcd}(a,b) = 1$, donc voici l'algorithme :

Algorithme . arith.py (2)

```
def nb_premiers_entre_eux(n,nbtirages) :
    i = 1
    nbpremiers = 0
    while i <= nbtirages :
        i = i+1
        a = random.randint(1,n)
        b = random.randint(1,n)
```

```
        if pgcd(a,b)==1 :
            nbpremiers = nbpremiers + 1
    return nbpremiers
```

On tire au hasard deux entiers a et b entre 1 et n et on effectue cette opération `nbtirages` fois. Par exemple entre 1 et 1000 si l'on effectue 10 000 tirage on trouve une probabilité mesurée par `nbpremiers/nbtirages` de 0,60... (les décimales d'après dépendent des tirages).
Lorsque n tend vers $+\infty$ alors $p_n \to \frac{6}{\pi^2} = 0.607927\ldots$ et on dit souvent que : «la probabilité que deux entiers tirés au hasard soient premiers entre eux est $\frac{6}{\pi^2}$.»

Commentaires sur les algorithmes récursifs :

- Les algorithmes récursifs ont souvent un code très court, et proche de la formulation mathématique lorsque l'on a une relation de récurrence.
- Selon le langage ou la fonction programmée il peut y avoir des problèmes de mémoire (si par exemple pour calculer 5! l'ordinateur a besoin de stocker 4! pour lequel il a besoin de stocker 3!...).
- Il est important de bien réfléchir à la condition initiale (qui est en fait celle qui termine l'algorithme) et à la récurrence sous peine d'avoir une fonction qui boucle indéfiniment !
- Il n'existe pas des algorithmes récursifs pour tout (voir par exemple les nombres premiers) mais ils apparaissent beaucoup dans les algorithmes de tris. Autre exemple : la dichotomie se programme très bien par une fonction récursive.

5.3. Nombres premiers

Les nombres premiers offrent peu de place aux algorithmes récursifs car il n'y a pas de lien de récurrence entre les nombres premiers.

Travaux pratiques 20

1. Écrire une fonction qui détecte si un nombre n est premier ou pas en testant s'il existe des entiers k qui divise n. (On se limitera aux entiers $2 \leqslant k \leqslant \sqrt{n}$, pourquoi ?).
2. Faire un algorithme pour le crible d'Eratosthène : écrire tous les entiers de 2 à n, conserver 2 (qui est premier) et barrer tous les multiples suivants de 2. Le premier nombre non barré (c'est 3) est premier. Barrer tous les multiples suivants de 3,...
3. Dessiner la spirale d'Ulam : on place les nombres entiers en spirale, et on colorie en rouge les nombres premiers.

$$\begin{array}{cccc} & & \cdots & \cdots \\ 5 & 4 & 3 & \vdots \\ 6 & 1 & 2 & 11 \\ 7 & 8 & 9 & 10 \end{array}$$

1. Si n n'est pas premier alors $n = a \times b$ avec $a, b \geqslant 2$. Il est clair que soit $a \leqslant \sqrt{n}$ ou bien $b \leqslant \sqrt{n}$ (sinon $n = a \times b > n$). Donc il suffit de tester les diviseurs $2 \leqslant k \leqslant \sqrt{n}$. D'où l'algorithme :

Algorithme . arith.py (3)

```
def est_premier(n) :
    if (n<=1) : return False
    k = 2
    while k*k <= n :
        if n%k==0 :
            return False
        else :
            k = k +1
    return True
```

Notez qu'il vaut mieux écrire la condition `k*k <= n` plutôt que `k <= sqrt(n)` : il est beaucoup plus rapide de calculer le carré d'un entier plutôt qu'extraire une racine carrée.

Nous avons utilisé un nouveau type de variable : un ***booléen*** est une variable qui ne peut prendre que deux états Vrai ou Faux (ici *True* or *False*, souvent codé 1 et 0). Ainsi `est_premier(13)` renvoie `True`, alors que `est_premier(14)` renvoie `False`.

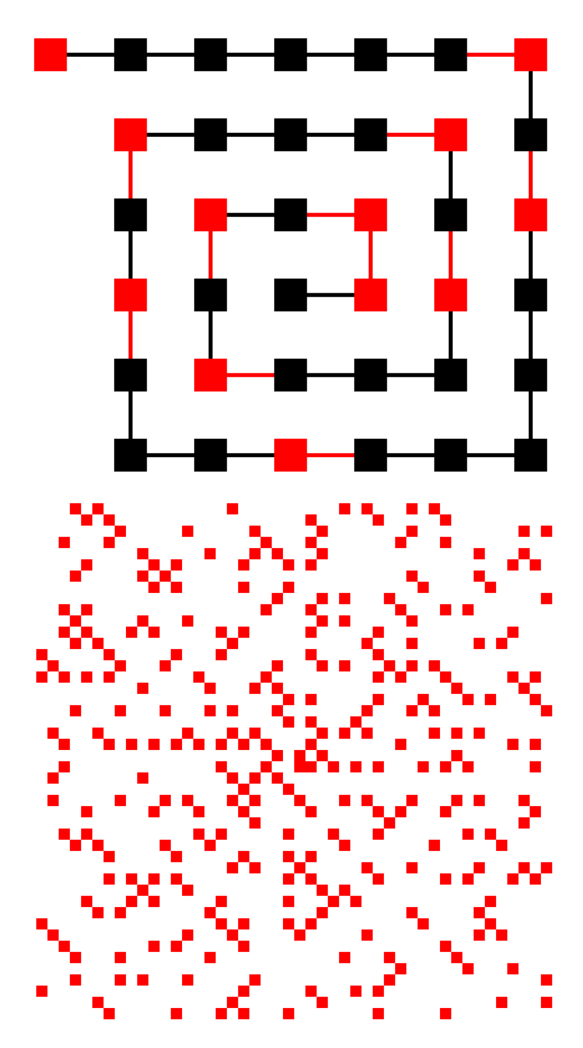
2. Pour le crible d'Eratosthène le plus dur est de trouver le bon codage de l'information.

Algorithme . arith.py (4)

```
def eratosthene(n) :
    liste_entiers = list(range(n+1))  # tous les entiers
    liste_entiers[1] = 0          # 1 n'est pas premier
    k = 2                         # on commence par les multiples de 2
    while k*k <= n :
        if liste_entiers[k]  != 0 : # si le nombre k n'est pas barré
            i = k                 # les i sont les multiples de k
            while i <= n-k :
                i = i+k
                liste_entiers[i] = 0  # multiples de k  : pas premiers
        k = k +1
    liste_premiers = [k for k in liste_entiers if k  !=0]  # efface les 0
    return liste_premiers
```

Ici on commence par faire un tableau contenant les entiers `[0,1,2,3,4,5,6,7,8,9,10,11,12,13,...]`. Pour signifier qu'un nombre n'est pas premier ou remplace l'entier par `0`. Comme 1 n'est pas un nombre premier : on le remplace par 0. Puis on fait une boucle, on part de 2 et on remplace tous les autres multiples de 2 par 0 : la liste est maintenant : `[0,0,2,3,0,5,0,7,0,9,0,11,0,13,...]`. Le premiers nombre après 2 est 3 c'est donc un nombre premier. (car s'il n'a aucun diviseur autre que 1 et lui-même car sinon il aurait été rayé). On garde 3 et remplace tous les autres multiples de 3 par 0. La liste est maintenant : `[0,0,2,3,0,5,0,7,0,0,0,11,0,13,...]`. On itère ainsi, à la fin on efface les zéros pour obtenir : `[2,3,5,7,11,13,...]`.

3. Pour la spirale d'Ulam la seule difficulté est de placer les entiers sur une spirale, voici le résultat.



À gauche le début de la spirale (de $n = 1$ à 37) en rouge les nombres premiers (en noir les nombres non premiers) ; à droite le motif obtenu jusqu'à de grandes valeurs (en blanc les nombres non premiers).

Mini-exercices

1. Écrire une version itérative et une version récursive pour les fonctions suivantes : (a) la somme des carrés des entiers de 1 à n ; (b) 2^n (sans utiliser d'exposant) ; (c) la partie entière d'un réel $x \geqslant 0$; (d) le quotient de la division euclidienne de a par b (avec $a \in \mathbb{N}$, $b \in \mathbb{N}^*$) ; (e) le reste de cette division euclidienne (sans utiliser les commandes % ni //).
2. Écrire une version itérative de la suite de Fibonacci.
3. Écrire une version itérative de l'algorithme d'Euclide. Faire une version qui calcule les coefficients de Bézout.
4. Écrire une fonction itérative, puis récursive, qui pour un entier n renvoie la liste de ses diviseurs. Dessiner une spirale d'Ulam, dont l'intensité de la couleur dépend du nombre de diviseurs.
5. Une suite de Syracuse est définie ainsi : partant d'un entier s'il est pair on le divise par deux, s'il est impair on le multiplie par 3 et on ajoute 1. On itère ce processus. Quelle conjecture peut-on faire sur cette suite ?

6. Dessiner le triangle de Pascal $\begin{smallmatrix} & & 1 & & \\ & 1 & & 1 & \\ 1 & & 2 & & 1 \\ & & \cdots & & \end{smallmatrix}$ Ensuite effacer tous les coefficients pairs (ou mieux : remplacer les coefficients pairs par un carré blanc et les coefficients impairs par un carré rouge). Quelle figure reconnaissez-vous ?

6. Polynômes – Complexité d'un algorithme

Nous allons étudier la complexité des algorithmes à travers l'exemple des polynômes.

6.1. Qu'est-ce qu'un algorithme ?

Qu'est ce qu'un algorithme ? Un algorithme est une succession d'instructions qui renvoie un résultat. Pour être vraiment un algorithme on doit justifier que le résultat retourné est ***exact*** (le programme fait bien ce que l'on souhaite) et ceci en un ***nombre fini d'étapes*** (cela renvoie le résultat en temps fini).
Maintenant certains algorithmes peuvent être plus rapides que d'autres. C'est souvent le temps de calcul qui est le principal critère, mais cela dépend du langage et de la machine utilisée. Il existe une manière plus mathématique de faire : la ***complexité*** d'un algorithme c'est le nombre d'opérations élémentaires à effectuer.
Ces opérations peuvent être le nombre d'opérations au niveau du processeur, mais pour nous ce sera le nombre d'additions $+$, le nombre de multiplications $\times$ à effectuer. Pour certains algorithmes la vitesse d'exécution n'est pas le seul paramètre mais aussi la taille de la mémoire occupée.

6.2. Polynômes

Travaux pratiques 21

On code un polynôme $a_0 + a_1X + \cdots + a_nX^n$ sous la forme d'une liste $[a_0, a_1, \ldots, a_n]$.

1. Écrire une fonction correspondant à la somme de deux polynômes. Calculer la complexité de cet algorithme (en terme du nombre d'additions sur les coefficients, en fonctions du degré des polynômes).
2. Écrire une fonction correspondant au produit de deux polynômes. Calculer la complexité de cet algorithme (en terme du nombre d'additions et de multiplications sur les coefficients).
3. Écrire une fonction correspondant au quotient et au reste de la division euclidienne de A par B où B est un polynôme unitaire (son coefficient de plus haut degré est 1). Majorer la complexité de cet algorithme (en terme du nombre d'additions et de multiplications sur les coefficients).

1. La seule difficulté est de gérer les indices, en particulier on ne peut appeler un élément d'une liste en dehors des indices où elle est définie. Une bonne idée consiste à commencer par définir une fonction `degre(poly)`, qui renvoie le degré du polynôme (attention au 0 non significatifs).

   Voici le code dans le cas simple où $\deg A = \deg B$:

Algorithme . polynome.py (1)

```
def somme(A,B) :            # si deg(A)=deg(B)
    C = []
    for i in range(0,degre(A)+1) :
        s = A[i]+B[i]
        C.append(s)
```

Calculons sa complexité, on suppose $\deg A \leqslant n$ et $\deg B \leqslant n$: il faut faire l'addition des coefficients $a_i + b_i$, pour i variant de 0 à n : donc la complexité est de $n+1$ additions (dans $\mathbb{Z}$ ou $\mathbb{R}$).

2. Pour le produit il faut se rappeler que si $A(X) = \sum_{i=0}^{m} a_i X^i$, $B(X) = \sum_{j=0}^{n} b_j X^j$ et $C = A \times B = \sum_{k=0}^{m+n} c_k X^k$ alors le k-ème coefficient de C est $c_k = \sum_{i+j=k} a_i \times b_j$. Dans la pratique on fait attention de ne pas accéder à des coefficients qui n'ont pas été définis.

Algorithme . polynome.py (2)

```
def produit(A,B) :
    C = []
    for k in range(degre(A)+degre(B)+1) :
        s = 0
        for i in range(k+1) :
            if (i <= degre(A)) and (k-i <= degre(B)) :
                s = s + A[i]*B[k-i]
        C.append(s)
    return C
```

Pour la complexité on commence par compter le nombre de multiplications (dans $\mathbb{Z}$ ou $\mathbb{R}$). Notons $m = \deg A$ et $n = \deg B$. Alors il faut multiplier les $m+1$ coefficients de A par les $n+1$ coefficients de B : il y a donc $(m+1)(n+1)$ multiplications.

Comptons maintenant les additions : les coefficients de $A \times B$ sont : $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $c_2 = a_2 b_0 + a_1 b_1 + a_2 b_0$,...

Nous utilisons l'astuce suivante : nous savons que le produit $A \times B$ est de degré $m+n$ donc a (au plus) $m+n+1$ coefficients. Partant de $(m+1)(n+1)$ produits, chaque addition regroupe deux termes, et nous devons arriver à $m+n+1$ coefficients. Il y a donc $(m+1)(n+1)-(m+n+1) = mn$ additions.

3. Pour la division euclidienne, le principe est de poser une division de polynôme. Par exemple pour $A = 2X^4 - X^3 - 2X^2 + 3X - 1$ et $B = X^2 - X + 1$.

$$
\begin{array}{r|l}
2X^4 - X^3 - 2X^2 + 3X - 1 & X^2 - X + 1 \\
- \quad 2X^4 - 2X^3 + 2X^2 & \\
\hline
X^3 - 4X^2 + 3X - 1 & 2X^2 + X - 3 \\
- \quad X^3 - X^2 + X & \\
\hline
-3X^2 + 2X - 1 & \\
- \quad -3X^2 + 3X - 3 & \\
\hline
-X + 2 &
\end{array}
$$

Alors on cherche quel monôme P_1 fait diminuer le degré de $A - P_1 B$, c'est $2X^2$ (le coefficient 2 est le coefficient dominant de A). On pose ensuite $R_1 = A - P_1 B = X^3 - 4X^2 + 3X - 1$, $Q_1 = 2X^2$, on recommence avec R_1 divisé par B, $R_2 = R_1 - P_2 B$ avec $P_2 = X$, $Q_2 = Q_1 + P_2$,... On arrête lorsque $\deg R_i < \deg B$.

Algorithme . polynome.py (3)

```
def division(A,B) :
    Q = [0]      # Quotient
    R = A        # Reste
    while (degre(R) >= degre(B)) :
        P = monome(R[degre(R)],degre(R)-degre(B))
        R = somme(R,produit(-P,B))
        Q = somme(Q,P)
    return Q,R
```

C'est une version un peu simplifiée du code : où $P = r_n X^{\deg R - \deg B}$ et où il faut remplacer $-P$ par $[-a_0, -a_1, \ldots]$. Si $A, B \in \mathbb{Z}[X]$ alors le fait que B soit unitaire implique que Q et R sont aussi à coefficients entiers.

Quelle est la complexité de la division euclidienne ? À chaque étape on effectue une multiplication de polynômes ($P_i \times B$) puis une addition de polynôme ($R_i - P_i B$) ; à chaque étape le degré de R_i diminue (au moins) de 1. Donc il y a au plus $\deg A - \deg B + 1$ étapes.

Mais dans la pratique c'est plus simple que cela. La multiplication $P_i \times B$ est très simple : car P_i est un monôme $P_i = p_i X^i$. Multiplier par X^i c'est juste un décalage d'indice (comme multiplier par 10^i en écriture décimale) c'est donc une opération négligeable. Il reste donc à multiplier les coefficients de B par p_i : il y a donc $\deg B + 1$ multiplications de coefficients. La soustraction aussi est assez simple on retire à R_i un multiple de B, donc on a au plus $\deg B + 1$ coefficients à soustraire : il y a à chaque étape $\deg B + 1$ additions de coefficients.

Bilan : si $m = \deg A$ et $n = \deg B$ alors la division euclidienne s'effectue en au plus $(m - n + 1)(m + 1)$ multiplications et le même nombre d'additions (dans $\mathbb{Z}$ ou $\mathbb{R}$).

6.3. Algorithme de Karatsuba

Pour diminuer la complexité de la multiplication de polynômes, on va utiliser un paradigme très classique de programmation : « diviser pour régner ». Pour cela, on va décomposer les polynômes

à multiplier P et Q de degrés strictement inférieurs à $2n$ en

$$P = P_1 + P_2 \cdot X^n \quad \text{et} \quad Q = Q_1 + Q_2 \cdot X^n$$

avec les degrés de P_1, P_2, Q_1 et Q_2 strictement inférieurs à n.

Travaux pratiques 22

1. Écrire une formule qui réduit la multiplication des polynômes P et Q de degrés strictement inférieurs à $2n$ en multiplications de polynômes de degrés strictement inférieurs à n.
2. Programmer un algorithme récursif de multiplication qui utilise la formule précédente. Quelle est sa complexité ?
3. On peut raffiner cette méthode avec la remarque suivante de Karatsuba : le terme intermédiaire de $P \cdot Q$ s'écrit

   $$P_1 \cdot Q_2 + P_2 \cdot Q_1 = (P_1 + P_2) \cdot (Q_1 + Q_2) - P_1Q_1 - P_2Q_2$$

   Comme on a déjà calculé P_1Q_1 et P_2Q_2, on échange deux multiplications et une addition (à gauche) contre une multiplication et quatre additions (à droite). Écrire une fonction qui réalise la multiplication de polynômes à la Karatsuba.
4. Trouver la formule de récurrence qui définit la complexité de la multiplication de Karatsuba. Quelle est sa solution ?

1. Il suffit de développer le produit $(P_1 + X^n P_2) \cdot (Q_1 + X^n Q_2)$:

   $$(P_1 + X^n P_2) \cdot (Q_1 + X^n Q_2) = P_1Q_1 + X^n \cdot (P_1Q_2 + P_2Q_1) + X^{2n} \cdot P_2Q_2$$

   On se ramène ainsi aux quatre multiplications P_1Q_1 , P_1Q_2 , P_2Q_1 et P_2Q_2 entre polynômes de degrés strictement inférieurs à n, plus deux multiplications par X^n et X^{2n} qui ne sont que des ajouts de zéros en tête de liste.
2. On sépare les deux étapes de l'algorithme : d'abord la découpe des polynômes (dans laquelle il ne faut pas oublier de donner n en argument car ce n'est pas forcément le milieu du polynôme, n doit être le même pour P et Q). Le découpage `P1,P2 = decoupe(P,n)` correspond à l'écriture $P = P_1 + X^n P_2$.

   Algorithme . polynome.py (4)

   ```
   def decoupe(P,n) :
       if (degre(P)<n) : return P, [0]
       else : return P[0 :n], P[n :]
   ```

   On a aussi besoin d'une fonction `produit_monome(P,n)` qui renvoie le polynôme $X^n \cdot P$ par un décalage. Voici la multiplication proprement dite avec les appels récursifs et leur combinaison.

Algorithme . polynome.py (5)

```
def produit_assez_rapide(P,Q) :
    p = degre(P)  ; q = degre(Q)
    if (p == 0) : return [P[0]*k for k in Q]  # Condition initiale : P=cst
    if (q == 0) : return [Q[0]*k for k in P]  # Condition initiale : Q=cst
    n = (max(p,q)+1)//2                       # demi-degré
    P1,P2 = decoupe(P,n)                      # decoupages
    Q1,Q2 = decoupe(Q,n)
    P1Q1 = produit_assez_rapide(P1,Q1)        # produits en petits degrés
    P2Q2 = produit_assez_rapide(P2,Q2)
    P1Q2 = produit_assez_rapide(P1,Q2)
    P2Q1 = produit_assez_rapide(P2,Q1)
    R1 = produit_monome(somme(P1Q2,P2Q1),n)  # décalages
    R2 = produit_monome(P2Q2,2*n)
    return somme(P1Q1,somme(R1,R2))           # sommes
```

La relation de récurrence qui exprime la complexité de cet algorithme est $C(n) = 4C(n/2) + O(n)$ et elle se résout en $C(n) = O(n^2)$. Voir la question suivante pour une méthode de résolution.

3.

Algorithme . polynome.py (6)

```
def produit_rapide(P,Q) :
    p = degre(P)  ; q = degre(Q)
    if (p == 0) : return [P[0]*k for k in Q]  # Condition initiale : P=cst
    if (q == 0) : return [Q[0]*k for k in P]  # Condition initiale : Q=cst
    n = (max(p,q)+1)//2                       # demi-degré
    P1,P2 = decoupe(P,n)                      # decoupages
    Q1,Q2 = decoupe(Q,n)
    P1Q1 = produit_rapide(P1,Q1)              # produits en petits degrés
    P2Q2 = produit_rapide(P2,Q2)
    PQ = produit_rapide(somme(P1,P2),somme(Q1,Q2))
    R1 = somme(PQ,somme([-k for k in P1Q1],[-k for k in P2Q2]))
    R1 = produit_monome(R1,n)                 # décalages
    R2 = produit_monome(P2Q2,2*n)
    return somme(P1Q1,somme(R1,R2))           # sommes
```

4. Notons $C(n)$ la complexité de la multiplication entre deux polynômes de degrés strictement inférieurs à n. En plus des trois appels récursifs, il y a des opérations linéaires : deux calculs de degrés, deux découpes en $n/2$ puis des additions : deux de taille $n/2$, une de taille n, une de taille $3n/2$ et une de taille $2n$. On obtient donc la relation de récurrence suivante :

$$C(n) = 3 \cdot C(n/2) + \gamma n$$

où $\gamma = \frac{15}{2}$. Une méthode de résolution est de poser $\alpha_\ell = \frac{C(2^\ell)}{3^\ell}$ qui vérifie $\alpha_\ell = \alpha_{\ell-1} + \gamma\left(\frac{2}{3}\right)^\ell$.

D'où on tire, puisque $\alpha_0 = C(1) = 1$,

$$\alpha_\ell = \gamma \sum_{k=1}^{\ell} \left(\frac{2}{3}\right)^k + \alpha_0 = 3\gamma\left(1 - \left(\frac{2}{3}\right)^{\ell+1}\right) + 1 - \gamma$$

puis pour $n = 2^\ell$:

$$C(n) = C(2^\ell) = 3^\ell \alpha_\ell = \gamma(3^{\ell+1} - 2^{\ell+1}) + (1-\gamma)3^\ell = O(3^\ell) = O(2^{\ell \frac{\ln 3}{\ln 2}}) = O(n^{\frac{\ln 3}{\ln 2}})$$

La complexité de la multiplication de Karatsuba est donc $O(n^{\frac{\ln 3}{\ln 2}}) \simeq O(n^{1.585})$.

6.4. Optimiser ses algorithmes

Voici quelques petites astuces pour accélérer l'écriture ou la vitesse des algorithmes :

- `k ** 3` au lieu de `k * k * k` (cela économise de la mémoire, une seule variable au lieu de 3) ;
- `k ** 2 <= n` au lieu de `k <= sqrt(n)` (les calculs avec les entiers sont beaucoup plus rapides qu'avec les réels) ;
- `x += 1` au lieu de `x = x +1` (gain de mémoire) ;
- `a,b = a+b, a-b` au lieu de `newa = a+b ; newb = a-b ; a = newa ; b = newb` (gain de mémoire, code plus court).

Cependant il ne faut pas que cela nuise à la lisibilité du code : il est important que quelqu'un puisse relire et modifier votre code. Le plus souvent c'est vous même qui modifierez les algorithmes qui vous avez écrits et vous serez ravi d'y trouver des commentaires clairs et précis !

Mini-exercices

1. Faire une fonction qui renvoie le pgcd de deux polynômes.
2. Comparer les complexités des deux méthodes suivantes pour évaluer un polynôme P en une valeur $x_0 \in \mathbb{R}$: $P(x_0) = a_0 + a_1 x_0 + \cdots + a_{n-1} x_0^{n-1} + a_n x_0^n$ et $P(x_0) = a_0 + x_0\Big(a_1 + x_0\big(a_2 + \cdots + x_0(a_{n-1} + a_n x_0)\big)\Big)$ (méthode de Horner).
3. Comment trouver le maximum d'une liste ? Montrer que votre méthode est de complexité minimale (en terme du nombre de comparaisons).
4. Soit $f : [a,b] \to \mathbb{R}$ une fonction continue vérifiant $f(a) \cdot f(b) \leqslant 0$. Combien d'itérations de la méthode de dichotomie sont nécessaires pour obtenir une racine de $f(x) = 0$ avec une précision inférieure à ε ?
5. Programmer plusieurs façons de calculer les coefficients du binôme de Newton $\binom{n}{k}$ et les comparer.
6. Trouver une méthode de calcul de 2^n qui utilise peu de multiplications. On commencera par écrire n en base 2.

Auteurs

Rédaction : Arnaud Bodin
Relecture : Jean-François Barraud
Remerciements à Lionel Rieg pour son tp sur l'algorithme de Karatsuba





1. Le chiffrement de César

1.1. César a dit...

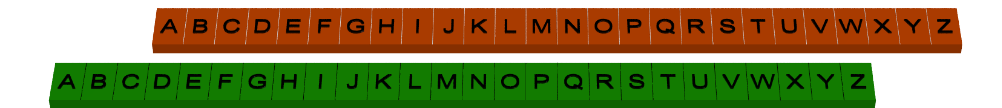
Jules César a-t-il vraiment prononcé la célèbre phrase :

DOHD MDFWD HVW

ou bien comme le disent deux célèbres Gaulois : « Ils sont fous ces romains ! ».
En fait César, pour ses communications importantes à son armée, cryptait ses messages. Ce que l'on appelle le chiffrement de César est un décalage des lettres : pour crypter un message, A devient D, B devient E, C devient F,...

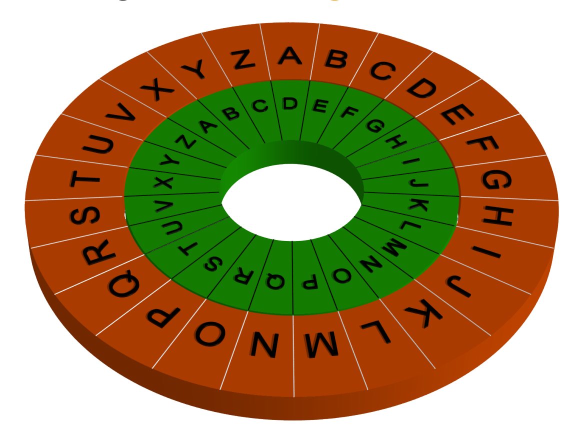
$$A \longmapsto D \quad B \longmapsto E \quad C \longmapsto F \quad \ldots \quad W \longmapsto Z \quad X \longmapsto A \quad Y \longmapsto B \quad Z \longmapsto C$$

Voici une figure avec l'alphabet d'origine en haut et en **rouge**, en correspondance avec l'alphabet pour le chiffrement en-dessous et en **vert**.



Nous adopterons la convention suivante, en **vert** c'est la partie du message à laquelle tout le monde a accès (ou qui pourrait être intercepté), c'est donc le message crypté. Alors qu'en **rouge** c'est la partie du message confidentiel, c'est le message en clair.

Pour prendre en compte aussi les dernières lettres de l'alphabet, il est plus judicieux de représenté l'alphabet sur un anneau. Ce décalage est un ***décalage circulaire*** sur les lettres de l'alphabet.



Pour déchiffrer le message de César, il suffit de décaler les lettres dans l'autre sens, D se déchiffre en A, E en B,...
Et la célèbre phrase de César est :

ALEA JACTA EST

qui traduite du latin donne « Les dés sont jetés ».

1.2. Des chiffres et des lettres

Il est plus facile de manipuler des nombres que des lettres, aussi nous passons à une formulation mathématique. Nous associons à chacune des 26 lettres de A à Z un nombre de 0 à 25. En termes mathématiques, nous définissons une bijection :

$$f : \{A,B,C,\ldots,Z\} \longrightarrow \{0,1,2,\ldots,25\}$$

par

$$A \longmapsto 0 \quad B \longmapsto 1 \quad C \longmapsto 2 \quad \ldots \quad Z \longmapsto 25$$

Ainsi "**A L E A**" devient "**0 11 4 0**".
Le chiffrement de César est un cas particulier de ***chiffrement mono-alphabétique***, c'est-à-dire un chiffrement lettre à lettre.
Quel est l'intérêt ? Nous allons voir que le chiffrement de César correspond à une opération mathématique très simple. Pour cela, rappelons la notion de congruence et l'ensemble $\mathbb{Z}/26\mathbb{Z}$.

1.3. Modulo

Soit $n \geqslant 2$ un entier fixé.

Définition 100

On dit que ***a est congru à b modulo n***, si n divise $b-a$. On note alors

$$a \equiv b \pmod n.$$

Pour nous $n = 26$. Ce qui fait que $28 \equiv 2 \pmod{26}$, car $28-2$ est bien divisible par 26. De même $85 = 3 \times 26 + 7$ donc $85 \equiv 7 \pmod{26}$.
On note $\mathbb{Z}/26\mathbb{Z}$ l'ensemble de tous les éléments de $\mathbb{Z}$ modulo 26. Cet ensemble peut par exemple être représenté par les 26 éléments $\{0,1,2,\ldots,25\}$. En effet, puisqu'on compte modulo 26 :

$$0,\ 1,\ 2,\ \ldots,\ 25, \quad \text{puis} \quad 26 \equiv 0,\ 27 \equiv 1,\ 28 \equiv 2, \ldots, \quad 52 \equiv 0,\ 53 \equiv 1, \ldots$$

et de même $-1 \equiv 25$, $-2 \equiv 24$,...

Plus généralement $\mathbb{Z}/n\mathbb{Z}$ contient n éléments. Pour un entier $a \in \mathbb{Z}$ quelconque, son ***représentant*** dans $\{0,1,2,\dots,n-1\}$ s'obtient comme le reste k de la division euclidienne de a par n : $a = bn+k$. De sorte que $a \equiv k \pmod n$ et $0 \leqslant k < n$.

De façon naturelle l'addition et la multiplication d'entiers se transposent dans $\mathbb{Z}/n\mathbb{Z}$.

Pour $a,b \in \mathbb{Z}/n\mathbb{Z}$, on associe $a+b \in \mathbb{Z}/n\mathbb{Z}$.
Par exemple dans $\mathbb{Z}/26\mathbb{Z}$, $15+13$ égale 2. En effet $15+13 = 28 \equiv 2 \pmod{26}$. Autre exemple : que vaut $133+64$? $133+64 = 197 = 7 \times 26 + 15 \equiv 15 \pmod{26}$. Mais on pourrait procéder différemment : tout d'abord $133 = 5 \times 26 + 3 \equiv 3 \pmod{26}$ et $64 = 2 \times 26 + 12 \equiv 12 \pmod{26}$. Et maintenant sans calculs : $133+64 \equiv 3+12 \equiv 15 \pmod{26}$.

On fait de même pour la multiplication : pour $a,b \in \mathbb{Z}/n\mathbb{Z}$, on associe $a \times b \in \mathbb{Z}/n\mathbb{Z}$.
Par exemple 3×12 donne 10 modulo 26, car $3 \times 12 = 36 = 1 \times 26 + 10 \equiv 10 \pmod{26}$. De même : $3 \times 27 = 81 = 3 \times 26 + 3 \equiv 3 \pmod{26}$. Une autre façon de voir la même opération est d'écrire d'abord $27 = 1 \pmod{26}$ puis $3 \times 27 \equiv 3 \times 1 \equiv 3 \pmod{26}$.

1.4. Chiffrer et déchiffrer

Le chiffrement de César est simplement une addition dans $\mathbb{Z}/26\mathbb{Z}$! Fixons un entier k qui est le décalage (par exemple $k=3$ dans l'exemple de César ci-dessus) et définissons la ***fonction de chiffrement de César de décalage*** k qui va de l'ensemble $\mathbb{Z}/26\mathbb{Z}$ dans lui-même :

$$C_k : \left\{ \begin{array}{ccc} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & x+k \end{array} \right.$$

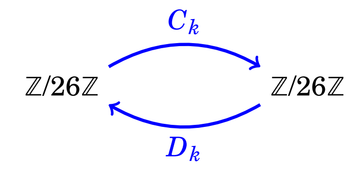
Par exemple, pour $k=3$: $C_3(0) = 3$, $C_3(1) = 4\dots$
Pour déchiffrer, rien de plus simple ! Il suffit d'aller dans l'autre sens, c'est-à-dire ici de soustraire. La ***fonction de déchiffrement de César de décalage*** k est

$$D_k : \left\{ \begin{array}{ccc} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & x-k \end{array} \right.$$

En effet, si 1 a été chiffré en 4, par la fonction C_3 alors $D_3(4) = 4-3 = 1$. On retrouve le nombre original. Mathématiquement, D_k est la bijection réciproque de C_k, ce qui implique que pour tout $x \in \mathbb{Z}/26\mathbb{Z}$:

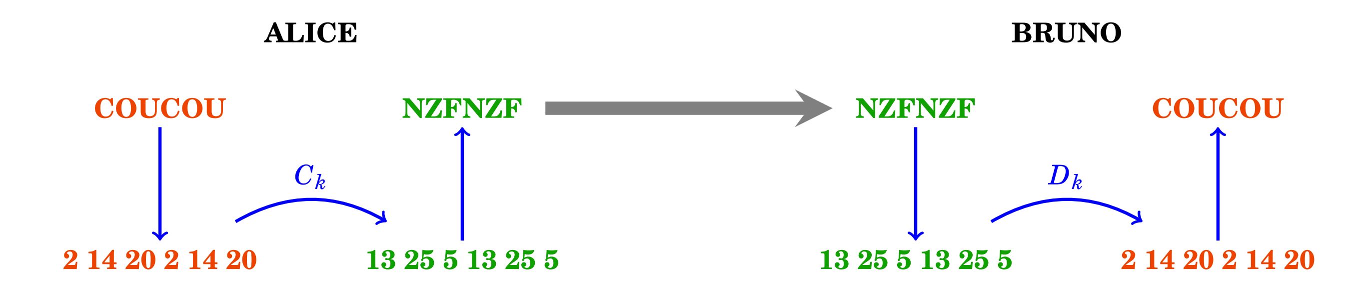
$$D_k\big(C_k(x)\big) = x$$

En d'autres termes, si x est un nombre, on applique la fonction de chiffrement pour obtenir le nombre crypté $y = C_k(x)$; ensuite la fonction de déchiffrement fait bien ce que l'on attend d'elle $D_k(y) = x$, on retrouve le nombre original x.



Une autre façon de voir la fonction de déchiffrement est de remarquer que $D_k(x) = C_{-k}(x)$. Par exemple $C_{-3}(x) = x + (-3) \equiv x + 23 \pmod{26}$.

Voici le principe du chiffrement : Alice veut envoyer des messages secrets à Bruno. Ils se sont d'abord mis d'accord sur une clé secrète k, par exemple $k = 11$. Alice veut envoyer le message "**COUCOU**" à Bruno. Elle transforme "**COUCOU**" en "**2 14 20 2 14 20**". Elle applique la fonction de chiffrement $C_{11}(x) = x + 11$ à chacun des nombres : "**13 25 5 13 25 5**" ce qui correspond au mot crypté "**NZFNZF**". Elle transmet le mot crypté à Bruno, qui selon le même principe applique la fonction de déchiffrement $D_{11}(x) = x - 11$.



Exemple 211

Un exemple classique est le "rot13" (pour rotation par un décalage de 13) :

$$C_{13}(x) = x + 13$$

et comme $-13 \equiv 13 \pmod{26}$ alors $D_{13}(x) = x + 13$. La fonction de déchiffrement est la même que la fonction de chiffrement !
Exemple : déchiffrez le mot "**PRFNE**".

Notons ici deux points importants pour la suite : tout d'abord nous avons naturellement considéré un mot comme une succession de lettres, et chaque opération de chiffrement et déchiffrement s'effectue sur un bloc d'une seule lettre. Ensuite nous avons vu que chiffrer un message est une opération mathématique (certes sur un ensemble un peu spécial).

1.5. Espace des clés et attaque

Combien existe-t-il de possibilités de chiffrement par la méthode de César ? Il y a 26 fonctions C_k différentes, $k = 0, 1, \ldots, 25$. Encore une fois, k appartient à $\mathbb{Z}/26\mathbb{Z}$, car par exemple les fonctions C_{29} et C_3 sont identiques. Le décalage k s'appelle la ***clé de chiffrement***, c'est l'information nécessaire pour crypter le message. Il y a donc 26 clés différentes et l'***espace des clés*** est $\mathbb{Z}/26\mathbb{Z}$.

Il est clair que ce chiffrement de César est d'une sécurité très faible. Si Alice envoie un message secret à Bruno et que Chloé intercepte ce message, il sera facile pour Chloé de le décrypter même si elle ne connaît pas la clé secrète k. L'attaque la plus simple pour Chloé est de tester ce que donne chacune des 26 combinaisons possibles et de reconnaître parmi ces combinaisons laquelle donne un message compréhensible.

1.6. Algorithmes

Les ordinateurs ont révolutionné la cryptographie et surtout le décryptage d'un message intercepté. Nous montrons ici, à l'aide du langage `Python` comment programmer et attaquer le chiffrement de César. Tout d'abord la fonction de chiffrement se programme en une seule ligne :

Algorithme . cesar.py (1)

```
def cesar_chiffre_nb(x,k) :
    return (x+k)%26
```

Ici `x` est un nombre de $\{0,1,\ldots,25\}$ et `k` est le décalage. `(x+k)%26` renvoie le reste modulo 26 de la somme `(x+k)`. Pour le décryptage, c'est aussi simple :

Algorithme . cesar.py (2)

```
def cesar_dechiffre_nb(x,k) :
    return (x-k)%26
```

Pour chiffrer un mot ou un phrase, il n'y a pas de problèmes théoriques, mais seulement des difficultés techniques :

- Un mot ou une phrase est une chaîne de caractères, qui en fait se comporte comme une liste. Si `mot` est une chaîne alors `mot[0]` est la première lettre, `mot[1]` la deuxième lettre... et la boucle `for lettre in mot :` permet de parcourir chacune des lettres.
- Pour transformer une lettre en un nombre, on utilise le code Ascii qui à chaque caractère associe un nombre, `ord(A)` vaut 65, `ord(B)` vaut 66... Ainsi `(ord(lettre) - 65)` renvoie le rang de la lettre entre 0 et 25 comme nous l'avons fixé dès le départ.
- La transformation inverse se fait par la fonction `char` : `char(65)` renvoie le caractère `A`, `char(66)` renvoie `B`...
- Pour ajouter une lettre à une liste, faites `maliste.append(lettre)`. Enfin pour transformer une liste de caractères en une chaîne, faites `"".join(maliste)`.

Ce qui donne :

Algorithme . cesar.py (3)

```
def cesar_chiffre_mot(mot,k) :
    message_code = []                   # Liste vide
    for lettre in mot :                  # Pour chaque lettre
        nb = ord(lettre)-65             # Lettre devient nb de 0 à 25
        nb_crypte = cesar_chiffre(nb,k)  # Chiffrement de César
        lettre_crypte = chr(nb_crypte+65)  # Retour aux lettres
        message_code.append(lettre_crypte) # Ajoute lettre au message
    message_code = "".join(message_code)   # Revient à chaine caractères
    return(message_code)
```

Pour l'attaque on parcourt l'intégralité de l'espace des clés : k varie de 0 à 25. Noter que pour décrypter les messages on utilise ici simplement la fonction de César avec la clé $-k$.

Algorithme . cesar.py (4)

```
def cesar_attaque(mot) :
    for k in range(26) :
        print(cesar_chiffre_mot(mot,-k))
    return None
```

2. Le chiffrement de Vigenère

2.1. Chiffrement mono-alphabétique

Principe

Nous avons vu que le chiffrement de César présente une sécurité très faible, la principale raison est que l'espace des clés est trop petit : il y a seulement 26 clés possibles, et on peut attaquer un message chiffré en testant toutes les clés à la main.
Au lieu de faire correspondre circulairement les lettres, on associe maintenant à chaque lettre une autre lettre (sans ordre fixe ou règle générale).
Par exemple :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	Q	B	M	X	I	T	E	P	A	L	W	H	S	D	O	Z	K	V	G	R	C	N	Y	J	U

Pour crypter le message

ETRE OU NE PAS ETRE TELLE EST LA QUESTION

on regarde la correspondance et on remplace la lettre **E** par la lettre **X**, puis la lettre **T** par la lettre **G**, puis la lettre **R** par la lettre **K**...
Le message crypté est alors :

XGKX DR SX OFV XGKX GXWWX XVG WF ZRXVGPDS

Pour le décrypter, en connaissant les substitutions, on fait l'opération inverse.

Avantage : nous allons voir que l'espace des clés est gigantesque et qu'il n'est plus question d'énumérer toutes les possibilités.
Inconvénients : la clé à retenir est beaucoup plus longue, puisqu'il faut partager la clé constituée des 26 lettres "FQBMX...". Mais surtout, nous allons voir que finalement ce protocole de chiffrement est assez simple à « craquer ».

Espace des clés

Mathématiquement, le choix d'une clé revient au choix d'une bijection de l'ensemble $\{A,B,\dots,Z\}$ vers le même ensemble $\{A,B,\dots,Z\}$. Il y a 26! choix possibles. En effet pour la lettre A de l'ensemble de départ, il y a 26 choix possibles (nous avions choisi F), pour B il reste 25 choix possibles (tout sauf F qui est déjà choisi), pour C il reste 24 choix... enfin pour Z il ne reste qu'une seule possibilité, la seule lettre non encore choisie. Au final il y a : $26\times25\times24\times\cdots\times2\times1$ soit 26! choix de clés. Ce qui fait environ 4×10^{26} clés. Il y a plus de clés différentes que de grains de sable sur Terre ! Si un ordinateur pouvait tester 1 000 000 de clés par seconde, il lui faudrait alors 12 millions d'années pour tout énumérer.

Attaque statistique

La principale faiblesse du chiffrement mono-alphabétique est qu'une même lettre est toujours chiffrée de la même façon. Par exemple, ici **E** devient **X**. Dans les textes longs, les lettres n'apparaissent pas avec la même fréquence. Ces fréquences varient suivant la langue utilisée. En français, les lettres les plus rencontrées sont dans l'ordre :

E S A I N T R U L O D C P M V Q G F H B X J Y Z K W

avec les fréquences (souvent proches et dépendant de l'échantillon utilisé) :

E	S	A	I	N	T	R	U	L	O	D
14.69%	8.01%	7.54%	7.18%	6.89%	6.88%	6.49%	6.12%	5.63%	5.29%	3.66%

Voici la méthode d'attaque : dans le texte crypté, on cherche la lettre qui apparaît le plus, et si le texte est assez long cela devrait être le chiffrement du **E**, la lettre qui apparaît ensuite dans l'étude des fréquences devrait être le chiffrement du **S**, puis le chiffrement du **A**... On obtient des morceaux de texte clair sous la forme d'une texte à trous et il faut ensuite deviner les lettres manquantes.

Par exemple, déchiffrons la phrase :

LHLZ HFQ BC HFFPZ WH YOUPFH MUPZH

On compte les apparitions des lettres :

H : 6 **F** : 4 **P** : 3 **Z** : 3

On suppose donc que le **H** crypte la lettre **E**, le **F** la lettre **S**, ce qui donne

*E** ES* ** ESS** *E ***SE ****E

D'après les statistiques **P** et **Z** devraient se décrypter en **A** et **I** (ou **I** et **A**). Le quatrième mot "**HFFPZ**", pour l'instant décrypté en "**ESS****", se complète donc en "**ESSAI**" ou "**ESSIA**". La première solution semble correcte ! Ainsi **P** crypte **A**, et **Z** crypte **I**. La phrase est maintenant :

*E*I ES* ** ESSAI *E ***ASE **AIE

En réfléchissant un petit peu, on décrypte le message :

CECI EST UN ESSAI DE PHRASE VRAIE

2.2. Le chiffrement de Vigenère

Blocs

L'espace des clés du chiffrement mono-alphabétique est immense, mais le fait qu'une lettre soit toujours cryptée de la même façon représente une trop grande faiblesse. Le chiffrement de Vigenère remédie à ce problème. On regroupe les lettres de notre texte par blocs, par exemple ici par blocs de longueur 4 :

CETTE PHRASE NE VEUT RIEN DIRE

devient

CETT EPHR ASEN EVEU TRIE NDIR E

(les espaces sont purement indicatifs, dans la première phrase ils séparent les mots, dans la seconde ils séparent les blocs).

Si k est la longueur d'un bloc, alors on choisit une clé constituée de k nombres de 0 à 25 : $(n_1, n_2, \ldots, n_k)$. Le chiffrement consiste à effectuer un chiffrement de César, dont le décalage dépend du rang de la lettre dans le bloc :

- un décalage de n_1 pour la première lettre de chaque bloc,
- un décalage de n_2 pour la deuxième lettre de chaque bloc,
- ...
- un décalage de n_k pour la k-ème et dernière lettre de chaque bloc.

Pour notre exemple, si on choisit comme clé $(3,1,5,2)$ alors pour le premier bloc "**CETT**" :

- un décalage de 3 pour **C** donne **F**,
- un décalage de 1 pour **E** donne **F**,
- un décalage de 5 pour le premier **T** donne **Y**,
- un décalage de 2 pour le deuxième **T** donne **V**.

Ainsi "**CETT**" de vient "**FFYV**". Vous remarquez que les deux lettres **T** ne sont pas cryptées par la même lettre et que les deux **F** ne cryptent pas la même lettre. On continue ensuite avec le deuxième bloc...

Mathématiques

L'élément de base n'est plus une lettre mais un ***bloc***, c'est-à-dire un regroupement de lettres. La fonction de chiffrement associe à un bloc de longueur k, un autre bloc de longueur k, ce qui donne en mathématisant les choses :

$$C_{n_1,n_2,\ldots,n_k} : \begin{cases} \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \times \cdots \times \mathbb{Z}/26\mathbb{Z} & \longrightarrow \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \times \cdots \times \mathbb{Z}/26\mathbb{Z} \\ (x_1,x_2,\ldots,x_k) & \longmapsto (x_1+n_1,x_2+n_2,\ldots,x_k+n_k) \end{cases}$$

Chacune des composantes de cette fonction est un chiffrement de César. La fonction de déchiffrement est juste $C_{-n_1,-n_2,\ldots,-n_k}$.

Espace des clés et attaque

Il y a 26^k choix possibles de clés, lorsque les blocs sont de longueur k. Pour des blocs de longueur $k=4$ cela en donne déjà 456 976, et même si un ordinateur teste toutes les combinaisons possibles sans problème, il n'est pas question de parcourir cette liste pour trouver le message en clair, c'est-à-dire celui qui est compréhensible !

Il persiste tout de même une faiblesse du même ordre que celle rencontrée dans le chiffrement mono-alphabétique : la lettre **A** n'est pas toujours cryptée par la même lettre, mais si deux lettres **A** sont situées à la même position dans deux blocs différents (comme par exemple "**ALPH ABET**") alors elles seront cryptées par la même lettre.

Une attaque possible est donc la suivante : on découpe notre message en plusieurs listes, les premières lettres de chaque bloc, les deuxièmes lettres de chaque bloc... et on fait une attaque statistique sur chacun de ces regroupements. Ce type d'attaque n'est possible que si la taille des blocs est petite devant la longueur du texte.

2.3. Algorithmes

Voici un petit algorithme qui calcule la fréquence de chaque lettre d'une phrase.

Algorithme . statistiques.py

```
def statistiques(phrase) :
    liste_stat = [0 for x in range(26)]      # Une liste avec des 0
    for lettre in phrase :                    # On parcourt la phrase
        i = ord(lettre)-65
        if 0 <= i < 26 :                      # Si c'est une vraie lettre
          liste_stat[i] = liste_stat[i] + 1
    return(liste_stat)
```

Et voici le chiffrement de Vigenère.

Algorithme . vigenere.py

```
def vigenere(mot,cle) :                       # Clé est du type [n_1,...,n_k]
    message_code = []
    k = len(cle)                              # Longueur de la clé
    i = 0                                     # Rang dans le bloc
    for lettre in mot :                        # Pour chaque lettre
        nomb = ord(lettre)-65                 # Lettre devient nb de 0 à 25
        nomb_code = (nomb+cle[i]) % 26        # Vigenère  : on ajoute n_i
        lettre_code = chr(nomb_code+65)       # On repasse aux lettres
        i=(i+1) % k                           # On passe au rang suivant
        message_code.append(lettre_code)      # Ajoute lettre au message
    message_code = "".join(message_code)      # Revient à chaine caractères
    return(message_code)
```

3. La machine Enigma et les clés secrètes

3.1. Un secret parfait

L'inconvénient des chiffrements précédents est qu'une même lettre est régulièrement chiffrée de la même façon, car la correspondance d'un alphabet à un ou plusieurs autres est fixée une fois pour toutes, ce qui fait qu'une attaque statistique est toujours possible. Nous allons voir qu'en changeant la correspondance à chaque lettre, il est possible de créer un chiffrement parfait !

Expliquons d'abord le principe à l'aide d'une analogie : j'ai choisi deux entiers m et c tels que $m+c=100$. Que vaut m ? C'est bien sûr impossible de répondre car il y a plusieurs possibilités : $0+100$, $1+99$, $2+98$,... Par contre, si je vous donne aussi c alors vous trouvez m immédiatement $m=100-c$.

Voici le principe du chiffrement : Alice veut envoyer à Bruno le message secret M suivant :

ATTAQUE LE CHATEAU

Alice a d'abord choisi une clé secrète C qu'elle a transmise à Bruno. Cette clé secrète est de la même longueur que le message (les espaces ne comptent pas) et composée d'entiers de 0 à 25, tirés au hasard. Par exemple C :

[4, 18, 2, 0, 21, 12, 18, 13, 7, 11, 23, 22, 19, 2, 16, 9]

Elle crypte la première lettre par un décalage de César donné par le premier entier : **A** est décalé de 4 lettres et devient donc **E**. La seconde lettre est décalée du second entier : le premier **T** devient **L**. Le second **T** est lui décalé de 2 lettres, il devient **V**. Le **A** suivant est décalé de 0 lettre, il reste **A**... Alice obtient un message chiffré X qu'elle transmet à Bruno :

ELVALGW YL NEWMGQD

Pour le décrypter, Bruno, qui connaît la clé, n'a qu'à faire le décalage dans l'autre sens.

Notez que deux lettres identiques (par exemples les **T**) n'ont aucune raison d'être cryptées de la même façon. Par exemple, les **T** du message initial sont cryptés dans l'ordre par un **L**, un **V** et un **M**.

Formalisons un peu cette opération. On identifie A avec 0, B avec 1, ..., Z avec 25. Alors le message crypté X est juste la "somme" du message M avec la clé secrète C, la somme s'effectuant lettre à

lettre, terme à terme, modulo 26.
Notons cette opération $M \oplus C = X$.

	A	T	T	A	Q	U	E	L	E	C	H	A	T	E	A	U
	0	19	19	0	16	20	4	11	4	2	7	0	19	4	0	20
⊕																
	4	18	2	0	21	12	18	13	7	11	23	22	19	2	16	9
=	4	11	21	0	11	6	22	24	11	13	4	22	12	6	16	3
	E	L	V	A	L	G	W	Y	L	N	E	W	M	G	Q	D

Bruno reçoit X et connaît C, il effectue donc $X \ominus C = M$.
Pourquoi ce système est-il inviolable ? Pour chacune des lettres, c'est exactement le même problème que trouver m, sachant que $m + c = x$ (où $x = 100$), mais sans connaître c. Toutes les possibilités pour m pourraient être juste. Et bien sûr, dès que l'on connaît c, la solution est triviale : $m = x - c$.
Il y a trois principes à respecter pour que ce système reste inviolable :

1. La longueur de la clé est égale à la longueur du message.
2. La clé est choisie au hasard.
3. La clé ne sert qu'une seule fois.

Ce système appelé "masque jetable" ou chiffrement de Vernam est parfait en théorie, mais sa mise en œuvre n'est pas pratique du tout ! Tout d'abord il faut que la clé soit aussi longue que le message. Pour un message court cela ne pose pas de problème, mais pour envoyer une image par exemple cela devient très lourd. Ensuite, il faut trouver un moyen sûr d'envoyer la clé secrète à son interlocuteur avant de lui faire parvenir le message. Et il faut recommencer cette opération à chaque message, ou bien se mettre d'accord dès le départ sur un ***carnet de clés*** : une longue liste de clés secrètes.
Pour justifier que ce système est vraiment inviolable voici une expérience amusante : Alice veut envoyer le message M ="**ATTAQUE LE CHATEAU**" à Bruno, elle choisit la clé secrète C=[4, 18, 2, 0,...] comme ci-dessus et obtient le message chiffré X="**ELVA**..." qu'elle transmet à Bruno.
Alice se fait kidnapper par Chloé, qui veut l'obliger à déchiffrer son message. Heureusement, Alice a anticipé les soucis : elle a détruit le message M, la clé secrète C et a créé un faux message M' et une fausse clé secrète C'. Alice fournit cette fausse clé secrète C' à Chloé, qui déchiffre le message par l'opération $X \ominus C'$ et elle trouve le message bien inoffensif M' :

RECETTE DE CUISINE

Alice est innocentée !
Comment est-ce possible ? Alice avait au préalable préparé un message neutre M' de même longueur que M et calculé la fausse clé secrète $C' = X \ominus M'$. Chloé a obtenu (par la contrainte) X et C', elle déchiffre le message ainsi

$$X \ominus C' = X \ominus (X \ominus M') = (X \ominus X) \oplus M' = M'$$

Chloé trouve donc le faux message.
Ici la fausse clé C' est :

[13, 7, 19, 22, 18, 13, 18, 21, 7, 11, 10, 14, 20, 24, 3, 25]

La première lettre du message chiffré est un **E**, en reculant de 13 lettres dans l'alphabet, elle se déchiffre en **R**...

3.2. La machine Enigma

Afin de s'approcher de ce protocole de chiffrement parfait, il faut trouver un moyen de générer facilement de longues clés, comme si elles avaient été générées au hasard. Nous allons étudier deux exemples utilisés en pratique à la fin du siècle dernier, une méthode électro-mécanique : la machine Enigma et une méthode numérique : le DES.
La machine Enigma est une machine électro-mécanique qui ressemble à une machine à écrire. Lorsque qu'une touche est enfoncée, des disques internes sont actionnés et le caractère crypté s'allume. Cette machine, qui sert aussi au déchiffrement, était utilisée pour les communications de l'armée allemande durant la seconde guerre mondiale. Ce que les Allemands ne savaient pas, c'est que les services secrets polonais et britanniques avaient réussi à percer les secrets de cette machine et étaient capables de déchiffrer les messages transmis par les allemands. Ce long travail d'études et de recherches a nécessité tout le génie d'Alan Turing et l'invention de l'ancêtre de l'ordinateur.

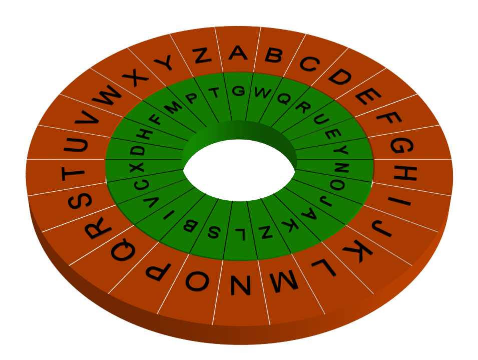


Nous symbolisons l'élément de base de la machine Enigma par deux anneaux :

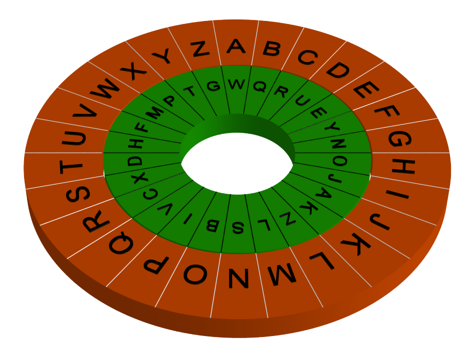
- Un anneau extérieur contenant l'alphabet "**ABCDE**..." symbolisant le clavier de saisie des messages. Cet anneau est fixe.
- Un anneau intérieur contenant un alphabet dans le désordre (sur la figure "**GWQRU**..."). Cet anneau est mobile et effectue une rotation à chaque touche tapée au clavier. Il représente la clé secrète.

Voici, dans ce cas, le processus de chiffrement du mot "**BAC**", avec la clé de chiffrement "**G**" :

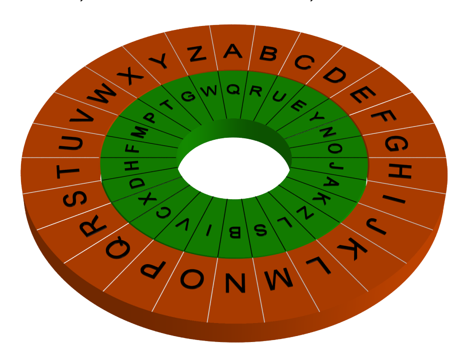
1. **Position initiale.** L'opérateur tourne l'anneau intérieur de sorte que le **A** extérieur et fixe soit en face du **G** intérieur (et donc **B** en face de **W**).



2. **Première lettre.** L'opérateur tape la première lettre du message : **B**, la machine affiche la correspondance **W**.
3. **Rotation.** L'anneau intérieur tourne de 1/26ème de tour, maintenant le **A** extérieur et fixe est en face du **W**, le **B** en face du **Q**,...



4. **Deuxième lettre.** L'opérateur tape la deuxième lettre du message **A**, la machine affiche la correspondance, c'est de nouveau **W**.
5. **Rotation.** L'anneau intérieur tourne de 1/26ème de tour, maintenant le **A** extérieur et fixe est en face du **Q**, le **B** en face du **R**, le **C** en face du **U**,...

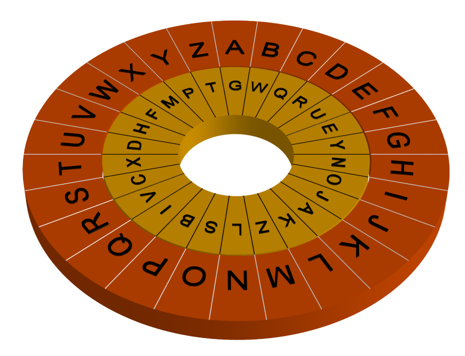


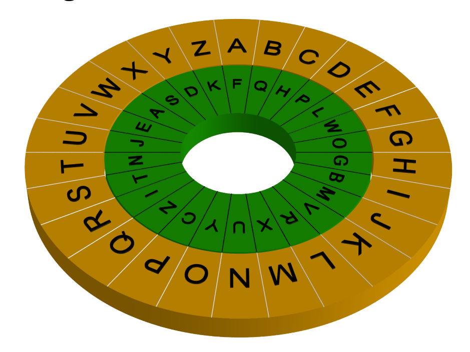
6. **Troisième lettre.** L'opérateur tape la troisième lettre du message **C**, la machine affiche la correspondance **U**.
7. **Rotation.** L'anneau intérieur effectue sa rotation.
8. **Message chiffré.** Le message crypté est donc "**WWU**"

Cette méthode de chiffrement est identique à un chiffrement de type Vigenère pour une clé de longueur 26. Il y a 26 clés différents à disposition avec un seul anneau intérieur et identifiées par lettre de la position initiale : **G**, **W**, **Q**... **T** correspondant aux alphabets : "**GWQ...PT**", "**WQR...TG**", "**QRU...GW**"...

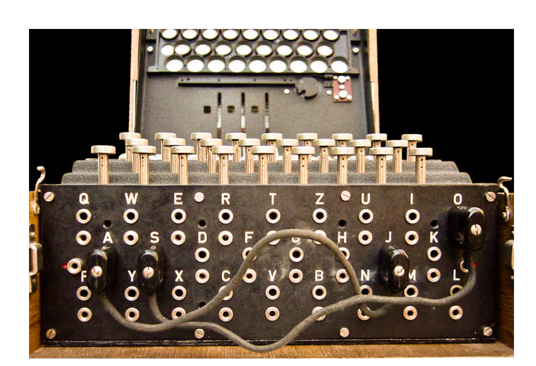
En fait, la machine Enigma était beaucoup plus sophistiquée, il n'y avait pas un mais plusieurs anneaux intérieurs. Par exemple pour deux anneaux intérieurs comme sur la figure : **B** s'envoie sur **W**, qui s'envoie sur **A** ; la lettre **B** est cryptée en **A**. Ensuite l'anneau intérieur numéro 1 effectue 1/26ème de tour. La lettre **A** s'envoie sur **W**, qui s'envoie sur **A** ; la lettre **A** est cryptée en

A. Lorsque l'anneau intérieur numéro 1 a fait une rotation complète (26 lettres ont été tapées) alors l'anneau intérieur numéro 2 effectue 1/26ème de tour. C'est comme sur un compteur kilométrique, lorsque le chiffre des kilomètres parcourt $0, 1, 2, 3, \ldots, 9$, alors au kilomètre suivant, le chiffre des kilomètres est 0 et celui des dizaines de kilomètres est augmenté d'une unité.





S'il y a trois anneaux, lorsque l'anneau intérieur 2 a fait une rotation complète, l'anneau intérieur 3 tourne de 1/26ème de tour. Il y a alors 26^3 clés différentes facilement identifiables par les trois lettres des positions initiales des anneaux.
Il fallait donc pour utiliser cette machine, d'abord choisir les disques (nos anneaux intérieurs) les placer dans un certain ordre, fixer la position initiale de chaque disque. Ce système était rendu largement plus complexe avec l'ajout de correspondances par fichage entre les lettres du clavier (voir photo). Le nombre de clés possibles dépassait plusieurs milliards de milliards !



3.3. La ronde des chiffres : DES

La machine Enigma génère mécaniquement un alphabet différent à chaque caractère crypté, tentant de se rapprocher d'un chiffrement parfait. Nous allons voir une autre méthode, cette fois numérique : le DES. Le DES (*Data Encryption Standard*) est un protocole de chiffrement par blocs. Il a été, entre 1977 et 2001, le standard de chiffrement pour les organisations du gouvernement des États-Unis et par extension pour un grand nombre de pays dans le monde.

Commençons par rappeler que l'objectif est de générer une clé aléatoire de grande longueur. Pour ne pas avoir à retenir l'intégralité de cette longue clé, on va la générer de façon pseudo-aléatoire à partir d'une petite clé.
Voyons un exemple élémentaire de suite pseudo-aléatoire.
Soit (u_n) la suite définie par la donnée de (a, b) et de u_0 et la relation de récurrence

$$u_{n+1} \equiv a \times u_n + b \pmod{26}.$$

Par exemple pour $a = 2$, $b = 5$ et $u_0 = 6$, alors les premiers termes de la suites sont :

6 17 13 5 15 9 23 25 3 11 1 7 19 17 13 5

Les trois nombres (a, b, u_0) représentent la clé principale et la suite des $(u_n)_{n\in\mathbb{N}}$ les clés secondaires. Avantages : à partir d'une clé principale on a généré une longue liste de clés secondaires. Inconvénients : la liste n'est pas si aléatoire que cela, elle se répète ici avec une période de longueur 12 : $17, 13, 5, \ldots, 17, 13, 5, \ldots$

Le système DES est une version sophistiquée de ce processus : à partir d'une clé courte et d'opérations élémentaires on crypte un message. Comme lors de l'étude de la machine Enigma, nous allons présenter une version très simplifiée de ce protocole afin d'en expliquer les étapes élémentaires.
Pour changer, nous allons travailler modulo 10. Lorsque l'on travaille par blocs, les additions se font *bit* par *bit*. Par exemple : $[1\ 2\ 3\ 4] \oplus [7\ 8\ 9\ 0] = [8\ 0\ 2\ 4]$ car ($1+7 \equiv 8 \pmod{10}$, $2+8 \equiv 0 \pmod{10}$,...)
Notre message est coupé en blocs, pour nos explications ce seront des blocs de longueur 8. La clé est de longueur 4.
Voici le message (un seul bloc) : $M = [1\ 2\ 3\ 4\ 5\ 6\ 7\ 8]$ et voici la clé : $C = [3\ 1\ 3\ 2]$.

Étape 0. Initialisation. On note $M_0 = M$ et on découpe M en une partie gauche et une partie droite

$$M_0 = [G_0 \parallel D_0] = [1\ 2\ 3\ 4 \parallel 5\ 6\ 7\ 8]$$

Étape 1. Premier tour. On pose

$$M_1 = [D_0 \parallel C \oplus \sigma(G_0)]$$

où σ est une permutation circulaire.
On effectue donc trois opérations pour passer de M_0 à M_1 :

1. On échange la partie droite et la partie gauche de M_0 :

$$M_0 \longmapsto [5\ 6\ 7\ 8 \parallel 1\ 2\ 3\ 4]$$

2. Sur la nouvelle partie droite, on permute circulairement les nombres :

$$\longmapsto [5\ 6\ 7\ 8 \parallel 2\ 3\ 4\ 1]$$

3. Puis on ajoute la clé secrète C à droite (ici $C = [3\ 1\ 3\ 2]$) :

$$\longmapsto [5\ 6\ 7\ 8 \parallel 5\ 4\ 7\ 3] = M_1$$

On va recommencer le même processus. Cela revient à appliquer la formule de récurrence, qui partant de $M_i = [G_i \parallel D_i]$, définit

$$M_{i+1} = [D_i \parallel C \oplus \sigma(G_i)]$$

Étape 2. Deuxième tour. On part de $M_1 = [5\ 6\ 7\ 8 \parallel 5\ 4\ 7\ 3]$.

1. On échange la partie droite et la partie gauche de M_0 :

$$M_0 \longmapsto [5\ 4\ 7\ 3 \parallel 5\ 6\ 7\ 8]$$

2. Sur la nouvelle partie droite, on permute circulairement les nombres.

$$\longmapsto [5\ 4\ 7\ 3 \parallel 6\ 7\ 8\ 5]$$

3. Puis on ajoute la clé secrète C à droite.

$$\longmapsto [5\ 4\ 7\ 3 \parallel 9\ 8\ 1\ 7] = M_2$$

On peut décider de s'arrêter après ce tour et renvoyer le message crypté $X = M_2 = [5\ 4\ 7\ 3\ 9\ 8\ 1\ 7]$. Comme chaque opération élémentaire est inversible, on applique un protocole inverse pour déchiffrer.
Dans le vrai protocole du DES, la clé principale est de taille 64 *bits*, il y a plus de manipulations sur le message et les étapes mentionnées ci-dessus sont effectuées 16 fois (on parle de tours). À chaque tour, une clé différente est utilisée. Il existe donc un préambule à ce protocole : générer 16 clés secondaires (de longueur 48 *bits*) à partir de la clé principale, ce qui se fait selon le principe de la suite pseudo-aléatoire (u_n) expliquée plus haut.

4. La cryptographie à clé publique

Les Grecs pour envoyer des messages secrets rasaient la tête du messager, tatouaient le message sur son crâne et attendaient que les cheveux repoussent avant d'envoyer le messager effectuer sa mission !
Il est clair que ce principe repose uniquement sur le secret de la méthode.

4.1. Le principe de Kerckhoffs

Cette méthode rudimentaire va à l'encontre du principe de Kerckhoffs. Le principe de Kerckhoffs s'énonce ainsi :

«La sécurité d'un système de chiffrement ne doit reposer que sur la clé.»

Cela se résume aussi par :

«L'ennemi peut avoir connaissance du système de chiffrement.»

Voici le texte original d'Auguste Kerckhoffs de 1883 «La cryptographie militaire» paru dans le *Journal des sciences militaires.*
Il traite notamment des enjeux de sécurité lors des correspondances :

> *«Il faut distinguer entre un système d'écriture chiffré, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux.»*

Le principe fondamental est le suivant :

> *«Dans le second cas, [. . .] il faut que* **le système n'exige pas le secret***, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.»*

Ce principe est novateur dans la mesure où intuitivement il semble opportun de dissimuler le maximum de choses possibles : clé et système de chiffrement utilisés. Mais l'objectif visé par Kerckhoffs est plus académique, il pense qu'un système dépendant d'un secret mais dont le mécanisme est connu de tous sera testé, attaqué, étudié, et finalement utilisé s'il s'avère intéressant et robuste.

4.2. Factorisations des entiers

Quels outils mathématiques répondent au principe de Kerckoffs ?

Un premier exemple est la toute simple multiplication ! En effet si je vous demande combien font 5×7, vous répondez 35. Si je vous demande de factoriser 35 vous répondez 5×7. Cependant ces deux questions ne sont pas du même ordre de difficulté. Si je vous demande de factoriser 1591, vous aller devoir faire plusieurs tentatives, alors que si je vous avais directement demandé de calculer 37×43 cela ne pose pas de problème.
Pour des entiers de plusieurs centaines de chiffres le problème de factorisation ne peut être résolu en un temps raisonnable, même pour un ordinateur. C'est ce problème asymétrique qui est à la base de la cryptographie RSA (que nous détaillerons plus tard) : connaître p et q apporte plus d'information utilisable que $p \times q$. Même si en théorie à partir de $p \times q$ on peut retrouver p et q, en pratique ce sera impossible.

Formalisons ceci avec la notion de complexité. La ***complexité*** est le temps de calculs (ou le nombre d'opérations élémentaires) nécessaire pour effectuer une opération.
Commençons par la complexité de l'addition : disons que calculer la somme de deux chiffres (par exemple $6+8$) soit de complexité 1 (par exemple 1 seconde pour un humain, 1 milliseconde pour un ordinateur). Pour calculer la somme de deux entiers à n chiffres, la complexité est d'ordre n (exemple : $1234+2323$, il faut faire 4 additions de chiffres, donc environ 4 secondes pour un humain).
La multiplication de deux entiers à n chiffres est de complexité d'ordre n^2. Par exemple pour multiplier 1234 par 2323 il faut faire 16 multiplications de chiffres (chaque chiffre de 1234 est à multiplier par chaque chiffre de 2323).
Par contre la meilleure méthode de factorisation connue est de complexité d'ordre $\exp(4n^{\frac{1}{3}})$ (c'est moins que $\exp(n)$, mais plus que n^d pour tout d, lorsque n tend vers $+\infty$).
Voici un tableau pour avoir une idée de la difficulté croissante pour multiplier et factoriser des nombres à n chiffres :

n	multiplication	factorisation
3	9	320
4	16	572
5	25	934
10	100	5 528
50	2 500	2 510 835
100	10 000	115 681 968
200	40 000	14 423 748 780

4.3. Fonctions à sens unique

Il existe bien d'autres situations mathématiques asymétriques : les ***fonctions à sens unique***. En d'autres termes, étant donnée une fonction f, il est possible connaissant x de calculer «facilement» $f(x)$; mais connaissant un élément de l'ensemble image de f, il est «difficile» ou impossible de trouver son antécédent.
Dans le cadre de la cryptographie, posséder une fonction à sens unique qui joue le rôle de chiffrement n'a que peu de sens. En effet, il est indispensable de trouver un moyen efficace afin de pouvoir déchiffrer les messages chiffrés. On parle alors de ***fonction à sens unique avec trappe secrète***.

Prenons par exemple le cas de la fonction f suivante :

$$f : x \longmapsto x^3 \pmod{100}.$$

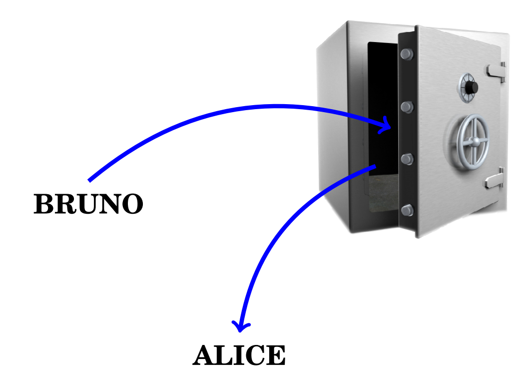
- Connaissant x, trouver $y = f(x)$ est facile, cela nécessite deux multiplications et deux divisions.
- Connaissant y image par f d'un élément x ($y = f(x)$), retrouver x est difficile.

Tentons de résoudre le problème suivant : trouver x tel que $x^3 \equiv 11 \pmod{100}$.
On peut pour cela :
- soit faire une recherche exhaustive, c'est-à-dire essayer successivement 1, 2, 3, ..., 99, on trouve alors :
$$71^3 = 357\,911 \equiv 11 \pmod{100},$$
- soit utiliser la trappe secrète : $y \longmapsto y^7 \pmod{100}$ qui fournit directement le résultat !
$$11^7 = 19\,487\,171 \equiv 71 \pmod{100}.$$

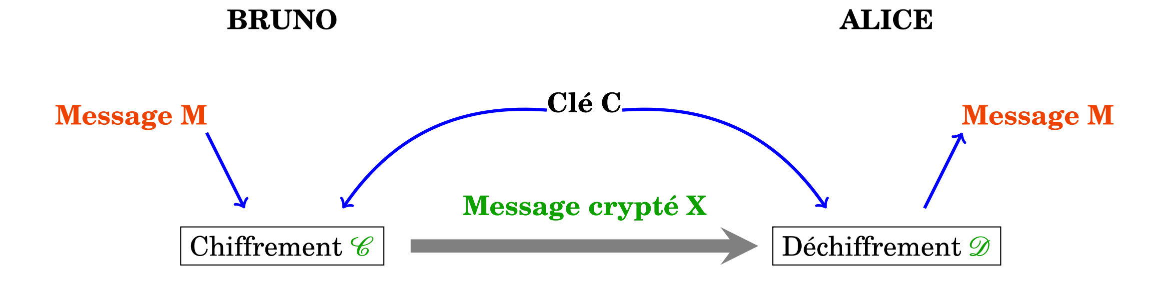
La morale est la suivante : le problème est dur à résoudre, sauf pour ceux qui connaissent la trappe secrète. (Attention, dans le cas de cet exemple, la fonction f n'est pas bijective.)

4.4. Chiffrement à clé privée

Petit retour en arrière. Les protocoles étudiés dans les chapitres précédents étaient des ***chiffrements à clé privée***. De façon imagée, tout se passe comme si Bruno pouvaient déposer son message dans un coffre fort pour Alice, Alice et Bruno étant les seuls à posséder la clé du coffre.

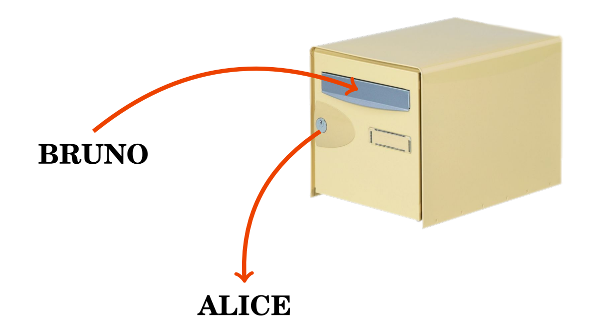


En effet, jusqu'ici, les deux interlocuteurs se partageaient une même clé qui servait à chiffrer (et déchiffrer) les messages. Cela pose bien sûr un problème majeur : Alice et Bruno doivent d'abord se communiquer la clé.

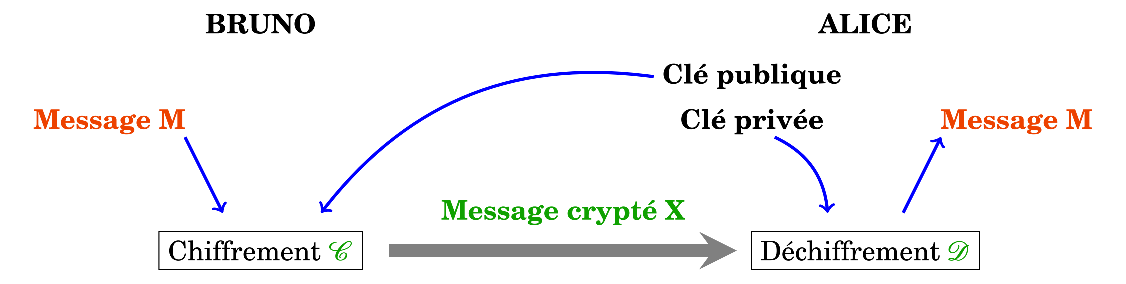


4.5. Chiffrement à clé publique

Les fonctions à sens unique à trappe donnent naissance à des protocoles de chiffrement à clé publique. L'association «clé» et «publique» peut paraître incongrue, mais il signifie que le principe de chiffrement est accessible à tous mais que le déchiffrement nécessite une clé qu'il faut bien sûr garder secrète.



De façon imagée, si Bruno veut envoyer un message à Alice, il dépose son message dans la boîte aux lettres d'Alice, seule Alice pourra ouvrir sa boîte et consulter le message. Ici la clé publique est symbolisée par la boîte aux lettre, tout le monde peut y déposer un message, la clé qui ouvre la boîte aux lettres est la clé privée d'Alice, que Alice doit conserver à l'abri.



En prenant appui sur l'exemple précédent, si le message initial est 71 et que la fonction f de chiffrement est connue de tous, le message transmis est 11 et le déchiffrement sera rapide si la trappe secrète 7 est connue du destinataire.
Les paramètres d'un protocole de ***chiffrement à clé publique*** sont donc :

- les fonctions de chiffrement et de déchiffrement : $\mathscr{C}$ et $\mathscr{D}$,
- la clé publique du destinataire qui va permettre de paramétrer la fonction $\mathscr{C}$,
- la clé privée du destinataire qui va permettre de paramétrer la fonction $\mathscr{D}$.

Dans le cadre de notre exemple Bruno souhaite envoyer un message à Alice, ces éléments sont :

- $\mathscr{C}$: $x \longmapsto x^?$ (mod 100) et $\mathscr{D}$: $x \longmapsto x^?$ (mod 100),
- **3** : la clé publique d'Alice qui permet de définir complètement la fonction de chiffrement :
$$\mathscr{C} : x \longmapsto x^3 \pmod{100},$$
- **7** : la clé privée d'Alice qui permet de définir complètement la fonction de déchiffrement :
$$\mathscr{D} : x \longmapsto x^7 \pmod{100}.$$

Dans la pratique, un chiffrement à clé publique nécessite plus de calculs et est donc assez lent, plus lent qu'un chiffrement à clé privée. Afin de gagner en rapidité, un protocole hybride peut être mis en place de la façon suivante :

- à l'aide d'un protocole de chiffrement à clé publique, Alice et Bruno échangent une clé,
- Alice et Bruno utilise cette clé dans un protocole de chiffrement à clé privée.

5. L'arithmétique pour RSA

Pour un entier n, sachant qu'il est le produit de deux nombres premiers, il est difficile de retrouver les facteurs p et q tels que $n = pq$. Le principe du chiffrement RSA, chiffrement à clé publique, repose sur cette difficulté.
Dans cette partie nous mettons en place les outils mathématiques nécessaires pour le calcul des clés publique et privée ainsi que les procédés de chiffrement et déchiffrement RSA.

5.1. Le petit théorème de Fermat amélioré

Nous connaissons le petit théorème de Fermat

Théorème 56. Petit théorème de Fermat

Si p est un nombre premier et $a \in \mathbb{Z}$ alors

$$\boxed{a^p \equiv a \pmod p}$$

et sa variante :

Corollaire 21

Si p ne divise pas a alors

$$\boxed{a^{p-1} \equiv 1 \pmod p}$$

Nous allons voir une version améliorée de ce théorème dans le cas qui nous intéresse :

Théorème 57. Petit théorème de Fermat amélioré

Soient p et q deux nombres premiers distincts et soit $n = pq$. Pour tout $a \in \mathbb{Z}$ tel que $\text{pgcd}(a,n) = 1$ alors :

$$\boxed{a^{(p-1)(q-1)} \equiv 1 \pmod n}$$

On note $\varphi(n) = (p-1)(q-1)$, la ***fonction d'Euler***. L'hypothèse $\text{pgcd}(a,n) = 1$ équivaut ici à ce que a ne soit divisible ni par p, ni par q. Par exemple pour $p = 5$, $q = 7$, $n = 35$ et $\varphi(n) = 4 \cdot 6 = 24$. Alors pour $a = 1,2,3,4,6,8,9,11,12,13,16,17,18,\dots$ on a bien $a^{24} \equiv 1 \pmod{35}$.

Démonstration

Notons $c = a^{(p-1)(q-1)}$. Calculons c modulo p :

$$c \equiv a^{(p-1)(q-1)} \equiv (a^{(p-1)})^{q-1} \equiv 1^{q-1} \equiv 1 \pmod p$$

où l'on appliquer le petit théorème de Fermat : $a^{p-1} \equiv 1 \pmod p$, car p ne divise pas a.
Calculons ce même c mais cette fois modulo q :

$$c \equiv a^{(p-1)(q-1)} \equiv (a^{(q-1)})^{p-1} \equiv 1^{p-1} \equiv 1 \pmod q$$

où l'on appliquer le petit théorème de Fermat : $a^{q-1} \equiv 1 \pmod q$, car q ne divise pas a.
Conclusion partielle : $c \equiv 1 \pmod p$ et $c \equiv 1 \pmod q$.

Nous allons en déduire que $c \equiv 1 \pmod{pq}$.
Comme $c \equiv 1 \pmod p$ alors il existe $\alpha \in \mathbb{Z}$ tel que $c = 1 + \alpha p$; comme $c \equiv 1 \pmod q$ alors il existe $\beta \in \mathbb{Z}$ tel que $c = 1 + \beta q$. Donc $c - 1 = \alpha p = \beta q$. De l'égalité $\alpha p = \beta q$, on tire que $p | \beta q$.
Comme p et q sont premiers entre eux (car ce sont des nombres premiers distincts) alors par le lemme de Gauss on en déduit que $p|\beta$. Il existe donc $\beta' \in \mathbb{Z}$ tel que $\beta = \beta' p$.
Ainsi $c = 1 + \beta q = 1 + \beta' pq$. Ce qui fait que $c \equiv 1 \pmod{pq}$, c'est exactement dire $a^{(p-1)(q-1)} \equiv 1 \pmod n$.

5.2. L'algorithme d'Euclide étendu

Nous avons déjà étudié l'algorithme d'Euclide qui repose sur le principe que $\text{pgcd}(a,b) = \text{pgcd}(b, a \pmod b)$.
Voici sa mise en œuvre informatique.

Algorithme . euclide.py (1)

```
def euclide(a,b) :
    while b !=0  :
        a , b = b , a % b
    return a
```

On profite que `Python` assure les affectations simultanées, ce qui pour nous correspond aux suites

$$\begin{cases} a_{i+1} &= b_i \\ b_{i+1} &\equiv a_i \pmod{b_i} \end{cases}$$

initialisée par $a_0 = a$, $b_0 = b$.
Nous avons vu aussi comment « remonter » l'algorithme d'Euclide à la main pour obtenir les coefficients de Bézout u, v tels que $au + bv = \text{pgcd}(a,b)$. Cependant il nous faut une méthode plus automatique pour obtenir ces coefficients, c'est l'***algorithme d'Euclide étendu***.
On définit deux suites (x_i), (y_i) qui vont aboutir aux coefficients de Bézout.
L'initialisation est :

$$x_0 = 1 \qquad x_1 = 0 \qquad y_0 = 0 \qquad y_1 = 1$$

et la formule de récurrence pour $i \geqslant 1$:

$$x_{i+1} = x_{i-1} - q_i x_i \qquad y_{i+1} = y_{i-1} - q_i y_i$$

où q_i est le quotient de la division euclidienne de a_i par b_i.

Algorithme . euclide.py (2)

```
def euclide_etendu(a,b) :
    x = 1  ; xx = 0
    y = 0  ; yy = 1
    while b  != 0  :
        q = a // b
        a , b = b , a % b
        xx , x = x - q*xx , xx
        yy , y = y - q*yy , yy
    return (a,x,y)
```

Cet algorithme renvoie d'abord le pgcd, puis les coefficients u, v tels que $au + bv = \text{pgcd}(a,b)$.

5.3. Inverse modulo n

Soit $a \in \mathbb{Z}$, on dit que $x \in \mathbb{Z}$ est un ***inverse de a modulo n*** si $\boxed{ax \equiv 1 \pmod n.}$
Trouver un inverse de a modulo n est donc un cas particulier de l'équation $ax \equiv b \pmod n$.

Proposition 120

- a admet un inverse modulo n si et seulement si a et n sont premiers entre eux.
- Si $au + nv = 1$ alors u est un inverse de a modulo n.

En d'autres termes, trouver un inverse de a modulo n revient à calculer les coefficients de Bézout associés à la paire (a,n).

Démonstration

La preuve est essentiellement une reformulation du théorème de Bézout :

$$\begin{aligned} \operatorname{pgcd}(a,n)=1 &\iff \exists u,v\in\mathbb{Z} \quad au+nv=1 \\ &\iff \exists u\in\mathbb{Z} \quad au\equiv 1 \pmod n \end{aligned}$$

Voici le code :

Algorithme . euclide.py (3)

```
def inverse(a,n) :
    c,u,v = euclide_etendu(a,n)     # pgcd et coeff. de Bézout
    if c  != 1  :             # Si pgcd différent de 1 renvoie 0
        return 0
    else  :
        return u % n                      # Renvoie l'inverse
```

5.4. L'exponentiation rapide

Nous aurons besoin de calculer rapidement des puissances modulo n. Pour cela il existe une méthode beaucoup plus efficace que de calculer d'abord a^k puis de le réduire modulo n. Il faut garder à l'esprit que les entiers que l'on va manipuler ont des dizaines voir des centaines de chiffres.

Voyons la technique sur l'exemple de $5^{11} \pmod{14}$. L'idée est de seulement calculer $5, 5^2, 5^4, 5^8$... et de réduire modulo n à chaque fois. Pour cela on remarque que $11 = 8+2+1$ donc

$$5^{11} = 5^8 \times 5^2 \times 5^1.$$

Calculons donc les $5^{2^i} \pmod{14}$:

$$\begin{aligned} &5 \equiv 5 \pmod{14} \\ &5^2 \equiv 25 \equiv 11 \pmod{14} \\ &5^4 \equiv 5^2 \times 5^2 \equiv 11 \times 11 \equiv 121 \equiv 9 \pmod{14} \\ &5^8 \equiv 5^4 \times 5^4 \equiv 9 \times 9 \equiv 81 \equiv 11 \pmod{14} \end{aligned}$$

à chaque étape est effectuée une multiplication modulaire. Conséquence :

$$5^{11} \equiv 5^8 \times 5^2 \times 5^1 \equiv 11 \times 11 \times 5 \equiv 11 \times 55 \equiv 11 \times 13 \equiv 143 \equiv 3 \pmod{14}.$$

Nous obtenons donc un calcul de $5^{11} \pmod{14}$ en 5 opérations au lieu de 10 si on avait fait $5 \times 5 \times 5 \cdots$.

Voici une formulation générale de la méthode. On écrit le développement de l'exposant k en base 2 : $(k_\ell,\dots,k_2,k_1,k_0)$ avec $k_i \in \{0,1\}$ de sorte que

$$k = \sum_{i=0}^{\ell} k_i 2^i.$$

On obtient alors

$$x^k = x^{\sum_{i=0}^{\ell} k_i 2^i} = \prod_{i=0}^{\ell} (x^{2^i})^{k_i}.$$

Par exemple 11 en base 2 s'écrit $(1,0,1,1)$, donc, comme on l'a vu :

$$5^{11} = (5^{2^3})^1 \times (5^{2^2})^0 \times (5^{2^1})^1 \times (5^{2^0})^1.$$

Voici un autre exemple : calculons $17^{154} \pmod{100}$. Tout d'abord on décompose l'exposant $k = 154$ en base 2 : $154 = 128 + 16 + 8 + 2 = 2^7 + 2^4 + 2^3 + 2^1$, il s'écrit donc en base 2 : $(1,0,0,1,1,0,1,0)$. Ensuite on calcule $17, 17^2, 17^4, 17^8, \dots, 17^{128}$ modulo 100.

$$\begin{aligned}
&17 \equiv 17 \pmod{100}\\
&17^2 \equiv 17 \times 17 \equiv 289 \equiv 89 \pmod{100}\\
&17^4 \equiv 17^2 \times 17^2 \equiv 89 \times 89 \equiv 7921 \equiv 21 \pmod{100}\\
&17^8 \equiv 17^4 \times 17^4 \equiv 21 \times 21 \equiv 441 \equiv 41 \pmod{100}\\
&17^{16} \equiv 17^8 \times 17^8 \equiv 41 \times 41 \equiv 1681 \equiv 81 \pmod{100}\\
&17^{32} \equiv 17^{16} \times 17^{16} \equiv 81 \times 81 \equiv 6561 \equiv 61 \pmod{100}\\
&17^{64} \equiv 17^{32} \times 17^{32} \equiv 61 \times 61 \equiv 3721 \equiv 21 \pmod{100}\\
&17^{128} \equiv 17^{64} \times 17^{64} \equiv 21 \times 21 \equiv 441 \equiv 41 \pmod{100}
\end{aligned}$$

Il ne reste qu'à rassembler :

$$17^{154} \equiv 17^{128} \times 17^{16} \times 17^8 \times 17^2 \equiv 41 \times 81 \times 41 \times 89 \equiv 3321 \times 3649 \equiv 21 \times 49 \equiv 1029 \equiv 29 \pmod{100}$$

On en déduit un algorithme pour le calcul rapide des puissances.

Algorithme . puissance.py

```
def puissance(x,k,n) :
    puiss = 1                      # Résultat
    while (k>0) :
        if k % 2 != 0  :            # Si k est impair (i.e. k_i=1)
            puiss = (puiss*x) % n
        x = x*x % n                # Vaut x, x^2, x^4,...
        k = k // 2
    return(puiss)
```

En fait Python sait faire l'exponentiation rapide : `pow(x,k,n)` pour le calcul de a^k modulo n, il faut donc éviter `(x ** k) % n` qui n'est pas adapté.

6. Le chiffrement RSA

Voici le but ultime de ce cours : la chiffrement RSA. Il est temps de relire l'introduction du chapitre « Arithmétique » pour s'apercevoir que nous sommes prêts !

Pour crypter un message on commence par le transformer en un –ou plusieurs– nombres. Les processus de chiffrement et déchiffrement font appel à plusieurs notions :

- *On choisit deux* **nombres premiers** *p et q que l'on garde secrets et on pose $n = p \times q$. Le principe étant que même connaissant n il est très difficile de retrouver p et q (qui sont des nombres ayant des centaines de chiffres).*
- *La clé secrète et la clé publique se calculent à l'aide de l'***algorithme d'Euclide** *et des* **coefficients de Bézout**.
- *Les calculs de cryptage se feront* **modulo** *n.*
- *Le déchiffrement fonctionne grâce à une variante du* **petit théorème de Fermat**.

Dans cette section, c'est Bruno qui veut envoyer un message secret à Alice. La processus se décompose ainsi :

1. Alice prépare une clé publique et une clé privée,
2. Bruno utilise la clé publique d'Alice pour crypter son message,
3. Alice reçoit le message crypté et le déchiffre grâce à sa clé privée.

6.1. Calcul de la clé publique et de la clé privée

Choix de deux nombres premiers

Alice effectue, une fois pour toute, les opérations suivantes (en secret) :

- elle choisit deux nombres premiers distincts p et q (dans la pratique ce sont de très grand nombres, jusqu'à des centaines de chiffres),
- Elle calcule $n = p \times q$,
- Elle calcule $\varphi(n) = (p-1) \times (q-1)$.

Exemple 1.

- $p = 5$ et $q = 17$
- $n = p \times q = 85$
- $\varphi(n) = (p-1) \times (q-1) = 64$

Vous noterez que le calcul de $\varphi(n)$ n'est possible que si la décomposition de n sous la forme $p \times q$ est connue. D'où le caractère secret de $\varphi(n)$ même si n est connu de tous.

Exemple 2.

- $p = 101$ et $q = 103$
- $n = p \times q = 10\,403$
- $\varphi(n) = (p-1) \times (q-1) = 10\,200$

Choix d'un exposant et calcul de son inverse

Alice continue :

- elle choisit un exposant e tel que $\text{pgcd}(e, \varphi(n)) = 1$,
- elle calcule l'inverse d de e module $\varphi(n)$: $d \times e \equiv 1 \pmod{\varphi(n)}$. Ce calcul se fait par l'algorithme d'Euclide étendu.

Exemple 1.

- Alice choisit par exemple $e = 5$ et on a bien $\text{pgcd}(e, \varphi(n)) = \text{pgcd}(5, 64) = 1$,

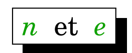
- Alice applique l'algorithme d'Euclide étendu pour calculer les coefficients de Bézout correspondant à $\text{pgcd}(e, \varphi(n)) = 1$. Elle trouve $5 \times 13 + 64 \times (-1) = 1$. Donc $5 \times 13 \equiv 1 \pmod{64}$ et l'inverse de e modulo $\varphi(n)$ est $d = 13$.

Exemple 2.

- Alice choisit par exemple $e = 7$ et on a bien $\text{pgcd}(e, \varphi(n)) = \text{pgcd}(7, 10\,200) = 1$,
- L'algorithme d'Euclide étendu pour $\text{pgcd}(e, \varphi(n)) = 1$ donne $7 \times (-1457) + 10\,200 \times 1 = 1$. Mais $-1457 \equiv 8743 \pmod{\varphi(n)}$, donc pour $d = 8743$ on a $d \times e \equiv 1 \pmod{\varphi(n)}$.

Clé publique

La ***clé publique*** d'Alice est constituée des deux nombres :



Et comme son nom l'indique Alice communique sa clé publique au monde entier.

Exemple 1. $n = 85$ et $e = 5$

Exemple 2. $n = 10\,403$ et $e = 7$

Clé privée

Alice garde pour elle sa ***clé privée*** :



Alice détruit en secret p, q et $\varphi(n)$ qui ne sont plus utiles. Elle conserve secrètement sa clé privée.

Exemple 1. $d = 13$

Exemple 2. $d = 8743$

6.2. Chiffrement du message

Bruno veut envoyer un message secret à Alice. Il se débrouille pour que son message soit un entier (quitte à découper son texte en bloc et à transformer chaque bloc en un entier).

Message

Le message est un entier m, tel que $0 \leqslant m < n$.

Exemple 1. Bruno veut envoyer le message $m = 10$.

Exemple 2. Bruno veut envoyer le message $m = 1234$.

Message chiffré

Bruno récupère la clé publique d'Alice : n et e avec laquelle il calcule, à l'aide de l'algorithme d'exponentiation rapide, le message chiffré :

$$\boxed{x \equiv m^e \pmod n}$$

Il transmet ce message x à Alice

Exemple 1. $m = 10$, $n = 85$ et $e = 5$ donc

$$x \equiv m^e \pmod n \equiv 10^5 \pmod{85}$$

On peut ici faire les calculs à la main :

$$\begin{aligned}
&10^2 \equiv 100 \equiv 15 \pmod{85}\\
&10^4 \equiv (10^2)^2 \equiv 15^2 \equiv 225 \equiv 55 \pmod{85}\\
&x \equiv 10^5 \equiv 10^4 \times 10 \equiv 55 \times 10 \equiv 550 \equiv 40 \pmod{85}
\end{aligned}$$

Le message chiffré est donc $x = 40$.

Exemple 2. $m = 1234$, $n = 10\,403$ et $e = 7$ donc

$$x \equiv m^e \pmod n \equiv 1234^7 \pmod{10\,403}$$

On utilise l'ordinateur pour obtenir que $x = 10\,378$.

6.3. Déchiffrement du message

Alice reçoit le message x chiffré par Bruno, elle le décrypte à l'aide de sa clé privée d, par l'opération :

$$\boxed{m \equiv x^d \pmod n}$$

qui utilise également l'algorithme d'exponentiation rapide.
Nous allons prouver dans le lemme 10, que par cette opération Alice retrouve bien le message original m de Bruno.

Exemple 1. $c = 40$, $d = 13$, $n = 85$ donc

$$x^d \equiv (40)^{13} \pmod{85}.$$

Calculons à la main $40^{13} \equiv \pmod{85}$ on note que $13 = 8+4+1$, donc $40^{13} = 40^8 \times 40^4 \times 40$.

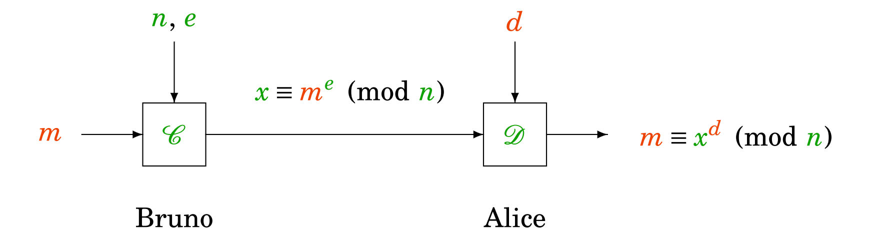
$$\begin{aligned}
&40^2 \equiv 1600 \equiv 70 \pmod{85}\\
&40^4 \equiv (40^2)^2 \equiv 70^2 \equiv 4900 \equiv 55 \pmod{85}\\
&40^8 \equiv (40^4)^2 \equiv 55^2 \equiv 3025 \equiv 50 \pmod{85}
\end{aligned}$$

Donc

$$x^d \equiv 40^{13} \equiv 40^8 \times 40^4 \times 40 \equiv 50 \times 55 \times 40 \equiv 10 \pmod{85}$$

qui est bien le message m de Bruno.

Exemple 2. $c = 10\,378$, $d = 8743$, $n = 10\,403$. On calcule par ordinateur $x^d \equiv (10\,378)^{8743} \pmod{10\,403}$ qui vaut exactement le message original de Bruno $m = 1234$.



6.4. Schéma

Clés d'Alice :

- publique : n, e
- privée : d

6.5. Lemme de déchiffrement

Le principe de déchiffrement repose sur le petit théorème de Fermat amélioré.

Lemme 10

Soit d l'inverse de e modulo $\varphi(n)$.

$$\text{Si } x \equiv m^e \pmod{n} \text{ alors } m \equiv x^d \pmod{n}.$$

Ce lemme prouve bien que le message original m de Bruno, chiffré par clé publique d'Alice (e, n) en le message x, peut-être retrouvé par Alice à l'aide de sa clé secrète d.

Démonstration

- Que d soit l'inverse de e modulo $\varphi(n)$ signifie $d \cdot e \equiv 1 \pmod{\varphi(n)}$. Autrement dit, il existe $k \in \mathbb{Z}$ tel que $d \cdot e = 1 + k \cdot \varphi(n)$.
- On rappelle que par le petit théorème de Fermat généralisé : lorsque m et n sont premiers entre eux
$$m^{\varphi(n)} \equiv m^{(p-1)(q-1)} \equiv 1 \pmod{n}$$
- **Premier cas** $\text{pgcd}(m, n) = 1$.
Notons $c \equiv m^e \pmod{n}$ et calculons x^d :
$$x^d \equiv (m^e)^d \equiv m^{e \cdot d} \equiv m^{1+k\cdot\varphi(n)} \equiv m \cdot m^{k\cdot\varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k \equiv m \cdot (1)^k \equiv m \pmod{n}$$
- **Deuxième cas** $\text{pgcd}(m, n) \neq 1$.
Comme n est le produit des deux nombres premiers p et q et que m est strictement plus petit que n alors si m et n ne sont pas premiers entre eux cela implique que p divise m ou bien q divise m (mais pas les deux en même temps). Faisons l'hypothèse $\text{pgcd}(m, n) = p$ et $\text{pgcd}(m, q) = 1$, le cas $\text{pgcd}(m, n) = q$ et $\text{pgcd}(m, p) = 1$ se traiterait de la même manière.
Étudions $(m^e)^d$ à la fois modulo p et modulo q à l'image de ce que nous avons fait dans la preuve du théorème de Fermat amélioré.
  - modulo p : $m \equiv 0 \pmod{p}$ et $(m^e)^d \equiv 0 \pmod{p}$ donc $(m^e)^d \equiv m \pmod{p}$,
  - modulo q : $(m^e)^d \equiv m \times (m^{\varphi(n)})^k \equiv m \times (m^{q-1})^{(p-1)k} \equiv m \pmod{q}$.

  Comme p et q sont deux nombres premiers distincts, ils sont premiers entre eux et on peut écrire comme dans la preuve du petit théorème de Fermat amélioré que
$$(m^e)^d \equiv m \pmod{n}$$

6.6. Algorithmes

La mise en œuvre est maintenant très simple. Alice choisit deux nombres premiers p et q et un exposant e.

Voici le calcul de la clé secrète :

Algorithme . rsa.py (1)

```
def cle_privee(p,q,e)  :
    n = p * q
    phi = (p-1)*(q-1)
    c,d,dd = euclide_etendu(e,phi)          # Pgcd et coeff de Bézout
    return(d % phi)                         # Bon représentant
```

Le chiffrement d'un message m est possible par tout le monde, connaissant la clé publique (n,e).

Algorithme . rsa.py (2)

```
def codage_rsa(m,n,e) :
    return pow(m,e,n)
```

Seule Alice peut déchiffrer le message crypté x, à l'aide de sa clé privée d.

Algorithme . rsa.py (3)

```
def decodage_rsa(x,n,d) :
    return pow(x,d,n)
```

Pour continuer...

Bibliographie commentée :

1. **Histoire des codes secrets** de Simon Singh, Le livre de Poche.
   Les codes secrets racontés comme un roman policier. Passionnant. Idéal pour les plus littéraires.
2. **Comprendre les codes secrets** de Pierre Vigoureux, édition Ellipses.
   Un petit livre très clair et très bien écrit, qui présente un panorama complet de la cryptographie sans rentrer dans les détails mathématiques. Idéal pour les esprits logiques.
3. **Codage et cryptographie** de Joan Gómez, édition Le Monde – Images des mathématiques.
   Un autre petit livre très clair et très bien, un peu de maths, des explications claires et des encarts historiques intéressants.
4. **Introduction à la cryptographie** de Johannes Buchmann, édition Dunod.
   Un livre d'un niveau avancé (troisième année de licence) pour comprendre les méthodes mathématiques de la cryptographie moderne. Idéal pour unifier les points de vue des mathématiques avec l'informatique.
5. **Algèbre - Première année** de Liret et Martinais, édition Dunod.
   Livre qui recouvre tout le programme d'algèbre de la première année, très bien adapté aux étudiants des l'université. Pas de cryptographie.

Auteurs

Arnaud Bodin
François Recher



20 Leçons de choses

Vidéo ■ partie 2. L'alphabet grec
Vidéo ■ partie 3. LATEX en cinq minutes
Vidéo ■ partie 4. Formules de trigonométrie : sinus, cosinus, tangente
Vidéo ■ partie 5. Formulaire : trigonométrie circulaire et hyperbolique
Vidéo ■ partie 6. Développements limités
Vidéo ■ partie 7. Primitives

1. Travailler avec les vidéos

Les vidéos ne remplacent pas les vrais cours. Cependant elle peuvent vous aider pour préparer, approfondir ou réviser vos connaissances. Nous vous offrons deux outils supplémentaires pour travailler : les polycopié de cours et les vidéos. Voici quelques conseils pour optimiser le visionnage.

1.1. Les vidéos

– Les deux outils de bases : ***papier & crayon***. Notez les points qui vous échappent pour pouvoir y revenir plus tard, faites des petits croquis, résolvez les mini-exercices,... Soyez actifs devant votre écran !
– Limitez-vous : ***une ou deux vidéos*** d'affilée c'est déjà beaucoup de travail. Il vaut mieux privilégier la régularité (par exemple une vidéo de cours par jour et deux vidéos d'exercices). Si vous enchaînez les vidéos comme une séance de cinéma, vous oublierez tout au bout de trois jours.
– Profitez des fonctions ***pause & retour en arrière*** pour prendre le temps de bien comprendre les notions, quitte à repassez la séquence trois fois. Les vidéos vont quatre à cinq fois plus vite que la « vraie vie » : *une vidéo de* 15 *minutes correspond à un cours d'une heure, un exercice corrigé en* $5-6$ *minutes en vidéo serait corrigé en une demi-heure en TD*.
– Il faut du ***temps*** et du ***travail***. Les mathématiques exigent pas mal d'efforts, mais cela vaut vraiment le coup. Tout le monde peut réussir, il n'y a pas besoin d'un don spécial ni d'être un génie des maths. Cependant ne vous leurrez pas, il y a des notions difficiles : bien sûr les profs et les vidéos sont là pour vous aider à les surmonter, mais l'apprentissage repose avant tout sur la qualité et la quantité de votre travail personnel.
– À titre d'exemple le chapitre *Nombres complexes* c'est 1h15 de cours en vidéos et aussi 1h15 d'exercices en vidéos. Cela correspond à 6 heures de cours dans la réalité et 12 heures de séances d'exercices (sur 2 à 3 semaines). Pensez aussi que les étudiants, en plus d'assister

aux cours et aux td, doivent fournir un travail personnel conséquent : à une heure de cours correspond une heure de travail personnel en plus ! Ainsi le chapitre *Nombres complexes* c'est plus de 30 heures de travail en tout et pas seulement 3 heures de visionnage.
Retenez donc le facteur 10 : **Une vidéo de** 12 **minutes c'est** 120 **minutes de travail.**

1.2. Pour les cours

Il faut :
- ***Recopier le cours*** au fur et à mesure du visionnage : écrire permet de mémoriser et d'adopter un rythme plus lent que celui de la vidéo.
- Travailler avec ***le poly*** qui contient plus de détails.
- ***Comprendre*** le cours.
- ***Apprendre*** le cours. Les définitions, les théorèmes et les propositions doivent être appris par cœur. Bien sûr une notion bien comprise est beaucoup plus facile à apprendre !
- Faire les ***mini-exercices***.
- Faire les fiches d'***exercices***.

1.3. Pour les exercices

- ***Chercher*** d'abord à résoudre l'exercice tout seul, sans regarder la correction (ni écrite, ni vidéo). Chercher demande du temps et de la persévérance. Cela permet de vérifier si l'on connaît bien son cours. Les exercices ne sont pas une suite d'astuces à retenir, mais un moyen de travailler par vous-même.
- Le ***lendemain*** seulement, vous pouvez regarder la correction.
- La vidéo de correction et la correction écrite sont complémentaires. Étudiez les deux.

1.4. Note aux collègues enseignants

Si vous êtes enseignants ces vidéos peuvent être utiles de plusieurs façons :
- Vous pouvez proposer les vidéos en compléments ou en révision de vos cours.
- Vous pouvez les proposer comme compléments ou comme sujet d'exposés à faire par les étudiants.
- Vous pouvez passez une vidéos dans vos cours : le support audiovisuel est mieux mémorisé qu'un cour classique, cela permet en plus de regagner l'attention des étudiants en diversifiant les types d'activités.
- Vous pouvez donner à vos étudiants à étudier seul un chapitre à l'avance, sur lequel vous revenez dans votre cours.

Vous trouverez des conseils efficaces dans le livre *Enseigner à l'université* de Markus Brauer. Si vous utilisez ces vidéos d'une façon ou d'une autre nous serions ravis d'avoir un retour de votre expérience !

1.5. D'autres sources pour travailler

Rien ne remplace un vrai prof dans une vraie salle de cours !

Voici deux livres papiers : *Algèbre* et *Analyse* de François Liret, Dominique Martinais aux éditions Dunod.
- Deux livres qui recouvrent le programme de première année.
- Adaptés aux étudiants de l'université.
- Un peu cher !

Voici un cours de première année accessible en ligne : *Cours concis de mathématiques – Première année* de Pierre Guillot.

- Cours concis et complet (370 pages).
- Adapté aux étudiants de l'université.
- Gratuit !

Et un livre accessible gratuitement en ligne *Cours de mathématiques – Math Sup* (attention gros fichier : 11 Mo) d'Alain Soyeur, François Capaces, Emmanuel Vieillard-Baron.

- Cours très complet (1200 pages !).
- Adapté aux élèves des classes prépas.
- Gratuit !

2. Alphabet grec

α		alpha
β		beta
γ	Γ	gamma
δ	Δ	delta
ε		epsilon
ζ		zeta
η		eta
θ	Θ	theta
ι		iota
κ		kappa
λ	Λ	lambda
μ		mu

ν		nu
ξ		xi
o		omicron
π	Π	pi
ρ, ϱ		rho
σ	Σ	sigma
τ		tau
υ		upsilon
ϕ, φ	Φ	phi
χ		chi
ψ	Ψ	psi
ω	Ω	omega

On rencontre aussi “nabla” ∇, l'opérateur de dérivée partielle ∂ (dites “d rond”), et aussi la première lettre de l'alphabet hébreu “aleph” $\aleph$.

3. Écrire des mathématiques : LaTeX en cinq minutes

3.1. Les bases

Pour écrire des mathématiques, il existe un langage pratique et universel, le langage LaTeX (prononcé [latek]). Il est utile pour rédiger des textes contenant des formules, mais aussi accepté sur certains blogs et vous permet d'écrire des maths dans un courriel ou un texto.

Une formule s'écrit entre deux dollars `$\pi^2$` qui donne π^2 ou entre double dollars si l'on veut la centrer sur une nouvelle ligne ; `$$\lim u_n = +\infty$$` affichera :

$$\lim u_n = +\infty$$

Dans la suite on omettra les balises dollars.

3.2. Premières commandes

Les exposants s'obtiennent avec la commande `^` et les indices avec `_` : a^2 s'écrit `a^2` ; u_n s'écrit `u_n` ; α_i^2 s'écrit `\alpha_i^2`. Les accolades `{ }` permettent de grouper du texte : `2^{10}` pour 2^{10} ; `a_{i,j}` pour $a_{i,j}$.
Il y a ensuite toute une liste de commandes (qui commencent par `\`) dont voici les plus utiles :

`\sqrt`	racine	$\sqrt{a}$	`\sqrt{a}`
		$\sqrt{1+\sqrt{2}}$	`\sqrt{1+\sqrt{2}}`
		$\sqrt[3]{x}$	`\sqrt[3]{x}`
`\frac`	fraction	$\frac{a}{b}$	`\frac{a}{b}`
		$\frac{\pi^3}{12}$	`\frac{\pi^3}{12}`
		$\frac{1}{2+\frac{3}{4}}$	`\frac{1}{2 + \frac{3}{4}}`
		$\gamma^{\frac{1}{n}}$	`\gamma^{\frac{1}{n}}`
`\lim`	limite	$\lim_{n\to+\infty} u_n = 0$	`\lim_{n \to +\infty} u_n = 0`
		$\lim_{x\to 0^+} f(x) < \varepsilon$	`\lim_{x \to 0^+} f(x) < \epsilon`
`\sum`	somme	$\sum_{i=1}^n \frac{1}{i}$	`\sum_{i=1}^n \frac{1}{i}`
		$\sum_{i\geqslant 0} a_i$	`\sum_{i \ge 0} a_i`
`\int`	intégrale	$\int_a^b \phi(t)dt$	`\int_a^b \phi(t) dt`

3.3. D'autres commandes

Voici d'autres commandes, assez naturelles pour les anglophones.

$f : E \to F$	`f : E \to F`
$+\infty$	`+\infty`
$a \leqslant 0$	`a \le 0`
$a > 0$	`a > 0`
$a \geqslant 1$	`a \ge 1`
δ	`\delta`
Δ	`\Delta`
$a \in E$	`a \in E`
$A \subset E$	`A \subset E`
$P \implies Q$	`P \implies Q`
$P \iff Q$	`P \iff Q`
$\forall$	`\forall`
$\exists$	`\exists`
$\cup$	`\cup`
$\cap$	`\cap`

3.4. Pour allez plus loin

Il est possible de créer ses propres commandes avec `\newcommand`. Par exemple avec l'instruction

`\newcommand{\Rr}{\mathbb{R}}`

vous définissez une nouvelle commande `\Rr` qui exécutera l'instruction `\mathbb{R}` et affichera donc $\mathbb{R}$.

Autre exemple, après avoir défini

`\newcommand{\monintegrale}{\int_0^{+\infty} \frac{\sin t}{t} dt}`

la commande `\monintegrale` affichera $\int_0^{+\infty} \frac{\sin t}{t} dt$.

Pour (beaucoup) plus de détails, consultez le manuel *Une courte (?) introduction à LaTeX*.

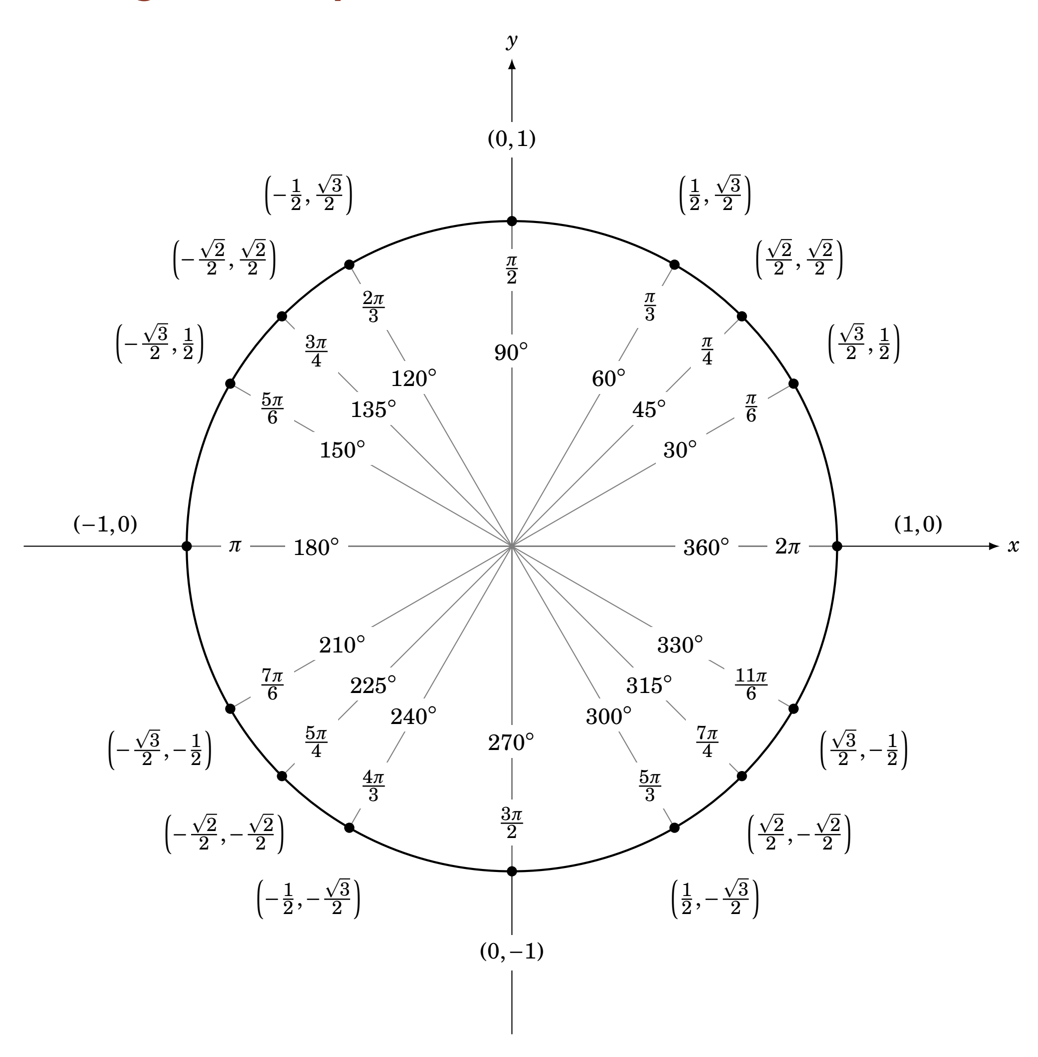
3.5. Mini-exercices

Écrire en LaTeX toutes ces formules (qui par ailleurs sont vraies !).

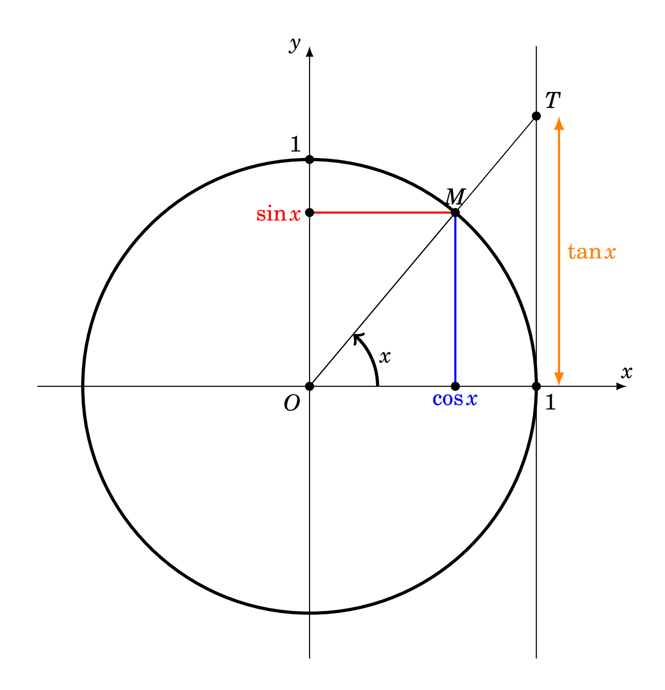
1. $\sqrt{a} - \sqrt{b} = \dfrac{a-b}{\sqrt{a}+\sqrt{b}}$
2. $\displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$
3. $\displaystyle\lim_{R\to+\infty} \int_{-R}^{+R} e^{-t^2} dt = \sqrt{\pi}$
4. $\forall \varepsilon > 0 \quad \exists \delta \geqslant 0 \quad (|x - x_0| < \delta \implies |\ln(x) - \ln(x_0)| < \varepsilon)$
5. $\displaystyle\sum_{k=0}^{+\infty} \frac{1}{16^k} \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right) = \pi$

4. Formules de trigonométrie : sinus, cosinus, tangente

4.1. Le cercle trigonométrique

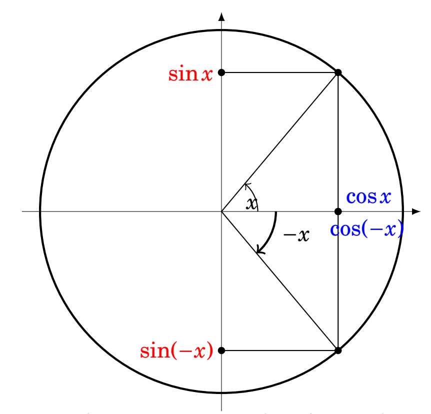


Voici le cercle trigonométrique (de rayon 1), le sens de lecture est l'inverse du sens des aiguilles d'une montre. Les angles remarquables sont marqués de 0 à 2π (en radian) et de 0° à 360°. Les coordonnées des points correspondant à ces angles sont aussi indiquées.



Le point M a pour coordonnées $(\cos x, \sin x)$. La droite (OM) coupe la droite d'équation $(x = 1)$ en T, l'ordonnée du point T est $\tan x$.
Les formules de base :

$$\cos^2 x + \sin^2 x = 1$$
$$\cos(x + 2\pi) = \cos x$$
$$\sin(x + 2\pi) = \sin x$$



Nous avons les formules suivantes :

$$\cos(-x) = \cos x$$
$$\sin(-x) = -\sin x$$

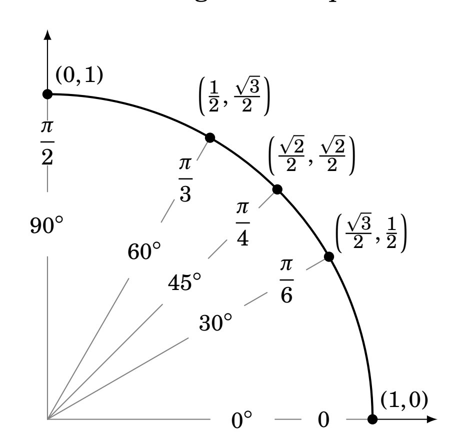
On retrouve graphiquement ces formules à l'aide du dessin des angles x et $-x$.

Il en est de même pour les formules suivantes :

$$\cos(\pi + x) = -\cos x \qquad \cos(\pi - x) = -\cos x \qquad \cos(\frac{\pi}{2} - x) = \sin x$$
$$\sin(\pi + x) = -\sin x \qquad \sin(\pi - x) = \sin x \qquad \sin(\frac{\pi}{2} - x) = \cos x$$

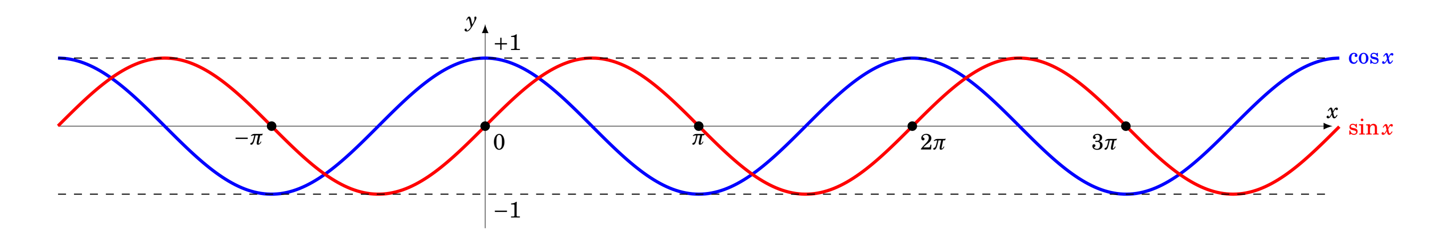
x	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
$\cos x$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0
$\sin x$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
$\tan x$	0	$\frac{1}{\sqrt{3}}$	1	$\sqrt{3}$	

Valeurs que l'on retrouve bien sur le cercle trigonométrique.

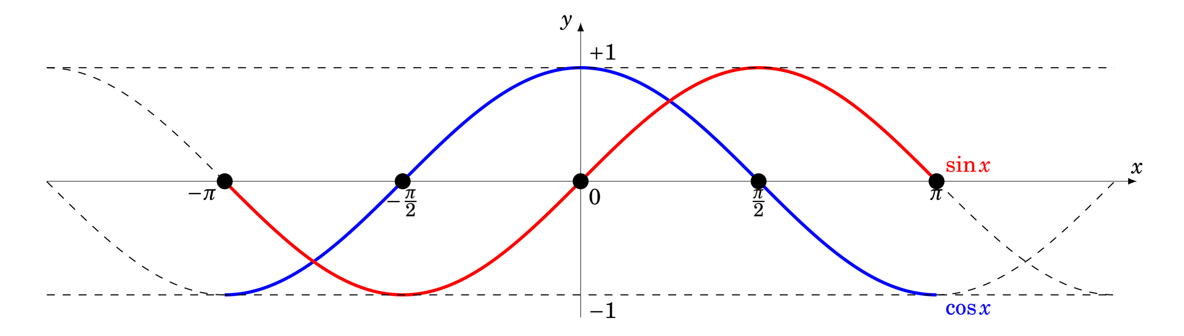


4.2. Les fonctions sinus, cosinus, tangente

La fonction cosinus est périodique de période 2π et elle paire (donc symétrique par rapport à l'axe des ordonnées). La fonction sinus est aussi périodique de période de 2π mais elle impaire (donc symétrique par rapport à l'origine).



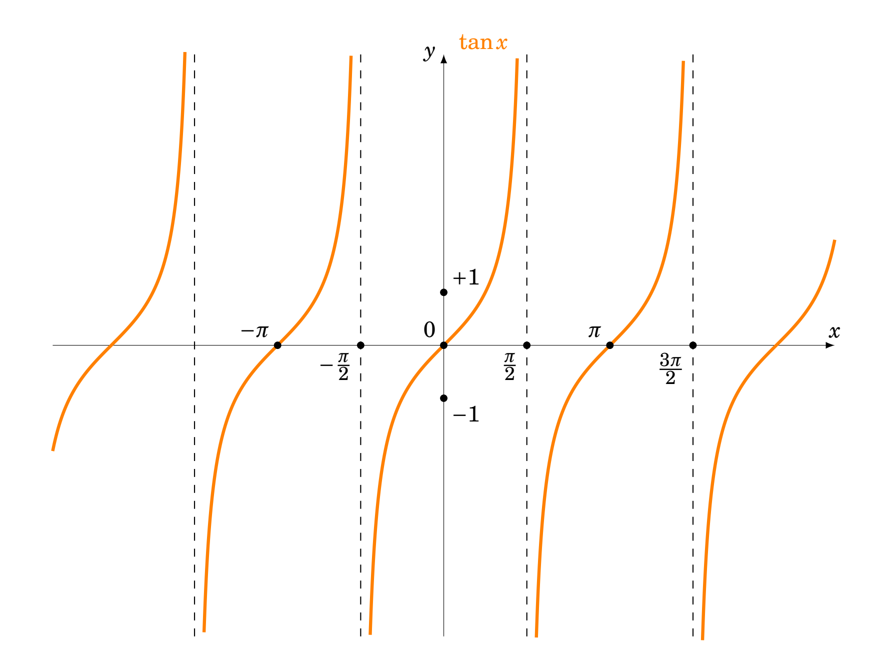
Voici un zoom sur l'intervalle $[-\pi, \pi]$.



Pour tout x n'appartenant pas à $\{\ldots, -\frac{\pi}{2}, \frac{\pi}{2}, \frac{3\pi}{2}, \frac{5\pi}{2}, \ldots\}$ la tangente est définie par

$$\tan x = \frac{\sin x}{\cos x}$$

La fonction $x \mapsto \tan x$ est périodique de période π ; c'est une fonction impaire.



Voici les dérivées :

$$\begin{aligned}\cos' x &= -\sin x\\ \sin' x &= \cos x\\ \tan' x &= 1+\tan^2 x = \frac{1}{\cos^2 x}\end{aligned}$$

4.3. Les formules d'additions

$$\begin{aligned}\cos(a+b) &= \cos a\cdot\cos b - \sin a\cdot\sin b\\ \sin(a+b) &= \sin a\cdot\cos b + \sin b\cdot\cos a\\ \tan(a+b) &= \frac{\tan a+\tan b}{1-\tan a\cdot\tan b}\end{aligned}$$

On en déduit immédiatement :

$$\begin{aligned}\cos(a-b) &= \cos a\cdot\cos b + \sin a\cdot\sin b\\ \sin(a-b) &= \sin a\cdot\cos b - \sin b\cdot\cos a\\ \tan(a-b) &= \frac{\tan a-\tan b}{1+\tan a\cdot\tan b}\end{aligned}$$

Il est bon de connaître par cœur les formules suivantes (faire $a = b$ dans les formules d'additions) :

$$\begin{aligned}\cos 2a &= 2\cos^2 a - 1\\ &= 1-2\sin^2 a\\ &= \cos^2 a - \sin^2 a\\ \sin 2a &= 2\sin a\cdot\cos a\\ \tan 2a &= \frac{2\tan a}{1-\tan^2 a}\end{aligned}$$

4.4. Les autres formules

Voici d'autres formules qui se déduisent des formules d'additions. Il n'est pas nécessaire de les connaître mais il faut savoir les retrouver en cas de besoin.

$$\begin{aligned}\cos a\cdot\cos b &= \frac{1}{2}\left[\cos(a+b)+\cos(a-b)\right]\\ \sin a\cdot\sin b &= \frac{1}{2}\left[\cos(a-b)-\cos(a+b)\right]\\ \sin a\cdot\cos b &= \frac{1}{2}\left[\sin(a+b)+\sin(a-b)\right]\end{aligned}$$

Les formules précédentes se reformulent aussi en :

$$\cos p + \cos q = 2\cos\frac{p+q}{2}\cdot\cos\frac{p-q}{2}$$
$$\cos p - \cos q = -2\sin\frac{p+q}{2}\cdot\sin\frac{p-q}{2}$$
$$\sin p + \sin q = 2\sin\frac{p+q}{2}\cdot\cos\frac{p-q}{2}$$
$$\sin p - \sin q = 2\sin\frac{p-q}{2}\cdot\cos\frac{p+q}{2}$$

Enfin les formules de la «tangente de l'arc moitié» permettent d'exprimer sinus, cosinus et tangente en fonction de $\tan\frac{x}{2}$.

$$\text{Avec}\quad t=\tan\frac{x}{2}\quad\text{on a}\quad\begin{cases}\cos x & =\frac{1-t^2}{1+t^2}\\ \sin x & =\frac{2t}{1+t^2}\\ \tan x & =\frac{2t}{1-t^2}\end{cases}$$

Ces formules sont utiles pour le calcul de certaines intégrales par changement de variable, en utilisant en plus la relation $dx=\dfrac{2dt}{1+t^2}$.

4.5. Mini-exercices

1. Montrer que $1+\tan^2 x=\frac{1}{\cos^2 x}$.
2. Montrer la formule d'addition de $\tan(a+b)$.
3. Prouver la formule pour $\cos a\cdot\cos b$.
4. Prouver la formule pour $\cos p+\cos q$.
5. Prouver la formule : $\sin x=\dfrac{2\tan\frac{x}{2}}{1+(\tan\frac{x}{2})^2}$.
6. Montrer que $\cos\frac{\pi}{8}=\frac{1}{2}\sqrt{\sqrt{2}+2}$. Calculer $\cos\frac{\pi}{16}$, $\cos\frac{\pi}{32}$,...
7. Exprimer $\cos(3x)$ en fonction $\cos x$; $\sin(3x)$ en fonction $\sin x$; $\tan(3x)$ en fonction $\tan x$.

5. Formulaire : trigonométrie circulaire et hyperbolique

Fonctions circulaires et hyperboliques

Propriétés trigonométriques *: remplacer* cos *par* ch *et* sin *par* i · sh.

$$\cos^2 x + \sin^2 x = 1$$

$$\cos(a+b) = \cos a \cdot \cos b - \sin a \cdot \sin b$$
$$\sin(a+b) = \sin a \cdot \cos b + \sin b \cdot \cos a$$
$$\tan(a+b) = \frac{\tan a + \tan b}{1 - \tan a \cdot \tan b}$$

$$\cos(a-b) = \cos a \cdot \cos b + \sin a \cdot \sin b$$
$$\sin(a-b) = \sin a \cdot \cos b - \sin b \cdot \cos a$$
$$\tan(a-b) = \frac{\tan a - \tan b}{1 + \tan a \cdot \tan b}$$

$$\cos 2a = 2\cos^2 a - 1 = 1 - 2\sin^2 a = \cos^2 a - \sin^2 a$$

$$\sin 2a = 2\sin a \cdot \cos a$$

$$\tan 2a = \frac{2\tan a}{1 - \tan^2 a}$$

$$\cos a \cdot \cos b = \frac{1}{2}\left[\cos(a+b) + \cos(a-b)\right]$$
$$\sin a \cdot \sin b = \frac{1}{2}\left[\cos(a-b) - \cos(a+b)\right]$$
$$\sin a \cdot \cos b = \frac{1}{2}\left[\sin(a+b) + \sin(a-b)\right]$$

$$\cos p + \cos q = 2\cos\frac{p+q}{2} \cdot \cos\frac{p-q}{2}$$
$$\cos p - \cos q = -2\sin\frac{p+q}{2} \cdot \sin\frac{p-q}{2}$$
$$\sin p + \sin q = 2\sin\frac{p+q}{2} \cdot \cos\frac{p-q}{2}$$
$$\sin p - \sin q = 2\sin\frac{p-q}{2} \cdot \cos\frac{p+q}{2}$$

$$\text{ch}^2 x - \text{sh}^2 x = 1$$

$$\text{ch}(a+b) = \text{ch}\, a \cdot \text{ch}\, b + \text{sh}\, a \cdot \text{sh}\, b$$
$$\text{sh}(a+b) = \text{sh}\, a \cdot \text{ch}\, b + \text{sh}\, b \cdot \text{ch}\, a$$
$$\text{th}(a+b) = \frac{\text{th}\, a + \text{th}\, b}{1 + \text{th}\, a \cdot \text{th}\, b}$$

$$\text{ch}(a-b) = \text{ch}\, a \cdot \text{ch}\, b - \text{sh}\, a \cdot \text{sh}\, b$$
$$\text{sh}(a-b) = \text{sh}\, a \cdot \text{ch}\, b - \text{sh}\, b \cdot \text{ch}\, a$$
$$\text{th}(a-b) = \frac{\text{th}\, a - \text{th}\, b}{1 - \text{th}\, a \cdot \text{th}\, b}$$

$$\text{ch}\, 2a = 2\,\text{ch}^2 a - 1 = 1 + 2\,\text{sh}^2 a = \text{ch}^2 a + \text{sh}^2 a$$

$$\text{sh}\, 2a = 2\,\text{sh}\, a \cdot \text{ch}\, a$$

$$\text{th}\, 2a = \frac{2\,\text{th}\, a}{1 + \text{th}^2 a}$$

$$\operatorname{ch} a \cdot \operatorname{ch} b = \frac{1}{2}\left[\operatorname{ch}(a+b)+\operatorname{ch}(a-b)\right]$$
$$\operatorname{sh} a \cdot \operatorname{sh} b = \frac{1}{2}\left[\operatorname{ch}(a+b)-\operatorname{ch}(a-b)\right]$$
$$\operatorname{sh} a \cdot \operatorname{ch} b = \frac{1}{2}\left[\operatorname{sh}(a+b)+\operatorname{sh}(a-b)\right]$$

$$\operatorname{ch} p + \operatorname{ch} q = 2\operatorname{ch}\frac{p+q}{2}\cdot\operatorname{ch}\frac{p-q}{2}$$
$$\operatorname{ch} p - \operatorname{ch} q = 2\operatorname{sh}\frac{p+q}{2}\cdot\operatorname{sh}\frac{p-q}{2}$$
$$\operatorname{sh} p + \operatorname{sh} q = 2\operatorname{sh}\frac{p+q}{2}\cdot\operatorname{ch}\frac{p-q}{2}$$
$$\operatorname{sh} p - \operatorname{sh} q = 2\operatorname{sh}\frac{p-q}{2}\cdot\operatorname{ch}\frac{p+q}{2}$$

avec $t = \tan \frac{x}{2}$ on a $\begin{cases} \cos x & = \frac{1-t^2}{1+t^2} \\ \sin x & = \frac{2t}{1+t^2} \\ \tan x & = \frac{2t}{1-t^2} \end{cases}$

avec $t = \text{th} \frac{x}{2}$ on a $\begin{cases} \text{ch}\, x & = \frac{1+t^2}{1-t^2} \\ \text{sh}\, x & = \frac{2t}{1-t^2} \\ \text{th}\, x & = \frac{2t}{1+t^2} \end{cases}$

Dérivées *: la multiplication par i n'est plus valable*

$$\cos' x = -\sin x$$
$$\sin' x = \cos x$$
$$\tan' x = 1 + \tan^2 x = \frac{1}{\cos^2 x}$$

$$\text{ch}' x = \text{sh}\, x$$
$$\text{sh}' x = \text{ch}\, x$$
$$\text{th}' x = 1 - \text{th}^2 x = \frac{1}{\text{ch}^2 x}$$

$$\text{Arccos}' x = \frac{-1}{\sqrt{1-x^2}} \quad (|x| < 1)$$
$$\text{Arcsin}' x = \frac{1}{\sqrt{1-x^2}} \quad (|x| < 1)$$
$$\text{Arctan}' x = \frac{1}{1+x^2}$$

$$\text{Argch}' x = \frac{1}{\sqrt{x^2-1}} \quad (x > 1)$$
$$\text{Argsh}' x = \frac{1}{\sqrt{x^2+1}}$$
$$\text{Argth}' x = \frac{1}{1-x^2} \quad (|x| < 1)$$

6. Formules de développements limités

Développements limités usuels *(au voisinage de 0)*

$$e^x = 1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!} + o(x^n) = \sum_{k=0}^{n}\frac{x^k}{k!} + o(x^n)$$

$$\cos x = 1-\frac{x^2}{2!}+\frac{x^4}{4!}-\cdots+(-1)^n\cdot\frac{x^{2n}}{(2n)!} + o(x^{2n+1}) = \sum_{k=0}^{n}(-1)^k\frac{x^{2k}}{(2k)!} + o(x^{2n+1})$$

$$\sin x = x-\frac{x^3}{3!}+\frac{x^5}{5!}-\cdots+(-1)^n\cdot\frac{x^{2n+1}}{(2n+1)!} + o(x^{2n+2}) = \sum_{k=0}^{n}(-1)^k\frac{x^{2k+1}}{(2k+1)!} + o(x^{2n+2})$$

$$\tan x = x+\frac{x^3}{3}+\frac{2}{15}x^5+\frac{17}{315}x^7 + o(x^8)$$

$$\operatorname{ch} x = 1+\frac{x^2}{2!}+\frac{x^4}{4!}+\cdots+\frac{x^{2n}}{(2n)!} + o(x^{2n+1}) = \sum_{k=0}^{n}\frac{x^{2k}}{(2k)!} + o(x^{2n+1})$$

$$\operatorname{sh} x = x+\frac{x^3}{3!}+\frac{x^5}{5!}+\cdots+\frac{x^{2n+1}}{(2n+1)!} + o(x^{2n+2}) = \sum_{k=0}^{n}\frac{x^{2k+1}}{(2k+1)!} + o(x^{2n+2})$$

$$\operatorname{th} x = x-\frac{x^3}{3}+\frac{2}{15}x^5-\frac{17}{315}x^7 + o(x^8)$$

$$\ln(1+x) = x-\frac{x^2}{2}+\frac{x^3}{3}-\cdots+(-1)^{n-1}\cdot\frac{x^n}{n} + o(x^n) = \sum_{k=1}^{n}(-1)^{k+1}\frac{x^k}{k} + o(x^n)$$

$$(1+x)^\alpha = 1+\alpha x+\frac{\alpha(\alpha-1)}{2!}x^2+\cdots+\frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}x^n + o(x^n) = \sum_{k=0}^{n}\binom{\alpha}{k}x^k + o(x^n)$$

$$\frac{1}{1+x} = 1-x+x^2-\cdots+(-1)^n x^n + o(x^n) = \sum_{k=0}^{n}(-1)^k x^k + o(x^n)$$

$$\frac{1}{1-x} = 1+x+x^2+\cdots+x^n + o(x^n) = \sum_{k=0}^{n}x^k + o(x^n)$$

$$\sqrt{1+x} = 1+\frac{x}{2}-\frac{1}{8}x^2-\cdots+(-1)^{n-1}\cdot\frac{1\cdot1\cdot3\cdot5\cdots(2n-3)}{2^n n!}x^n + o(x^n)$$

$$\frac{1}{\sqrt{1+x}} = 1-\frac{x}{2}+\frac{3}{8}x^2-\cdots+(-1)^n\cdot\frac{1\cdot3\cdot5\cdots(2n-1)}{2^n n!}x^n + o(x^n)$$

$$\arccos x = \frac{\pi}{2}-x-\frac{1}{2}\frac{x^3}{3}-\frac{1\cdot3}{2\cdot4}\frac{x^5}{5}-\cdots-\frac{1\cdot3\cdot5\cdots(2n-1)}{2\cdot4\cdot6\cdots(2n)}\frac{x^{2n+1}}{2n+1} + o(x^{2n+2})$$

$$\arcsin x = x+\frac{1}{2}\frac{x^3}{3}+\frac{1\cdot3}{2\cdot4}\frac{x^5}{5}+\cdots+\frac{1\cdot3\cdot5\cdots(2n-1)}{2\cdot4\cdot6\cdots(2n)}\frac{x^{2n+1}}{2n+1} + o(x^{2n+2})$$

$$\arctan x = x-\frac{x^3}{3}+\frac{x^5}{5}+\cdots+(-1)^n\cdot\frac{x^{2n+1}}{2n+1} + o(x^{2n+2})$$

7. Formulaire : primitives

Primitives usuelles

C désigne une constante arbitraire. Les intervalles sont à préciser.

$$\int e^{\alpha t}\,dt = \frac{e^{\alpha t}}{\alpha} + C \quad (\alpha \in \mathbb{C}^*)$$

$$\int t^{\alpha}\,dt = \frac{t^{\alpha+1}}{\alpha+1} + C \quad (\alpha \neq -1)$$

$$\int \frac{dt}{1+t^2} = \text{Arctan}\, t + C$$

$$\int \frac{dt}{\sqrt{1-t^2}} = \text{Arcsin}\, t + C$$

$$\int \cos t\,dt = \sin t + C$$

$$\int \sin t\,dt = -\cos t + C$$

$$\int \frac{dt}{\cos^2 t} = \tan t + C$$

$$\int \frac{dt}{\sin^2 t} = -\text{cotan}\, t + C$$

$$\int \frac{dt}{\cos t} = \ln\left|\tan\left(\frac{t}{2}+\frac{\pi}{4}\right)\right| + C$$

$$\int \frac{dt}{\sin t} = \ln\left|\tan\frac{t}{2}\right| + C$$

$$\int \tan t\,dt = -\ln|\cos t| + C$$

$$\int \text{cotan}\, t\,dt = \ln|\sin t| + C$$

$$\int \frac{dt}{t} = \ln|t| + C$$

$$\int \frac{dt}{1-t^2} = \frac{1}{2}\ln\left|\frac{1+t}{1-t}\right| + C$$

$$\int \frac{dt}{\sqrt{t^2+\alpha}} = \ln\left|t+\sqrt{t^2+\alpha}\right| + C$$

$$\int \text{ch}\, t\,dt = \text{sh}\, t + C$$

$$\int \text{sh}\, t\,dt = \text{ch}\, t + C$$

$$\int \frac{dt}{\text{ch}^2 t} = \text{th}\, t + C$$

$$\int \frac{dt}{\text{sh}^2 t} = -\text{coth}\, t + C$$

$$\int \frac{dt}{\text{ch}\, t} = 2\text{Arctan}\, e^t + C$$

$$\int \frac{dt}{\text{sh}\, t} = \ln\left|\text{th}\,\frac{t}{2}\right| + C$$

$$\int \text{th}\, t\,dt = \ln(\text{ch}\, t) + C$$

$$\int \text{coth}\, t\,dt = \ln|\text{sh}\, t| + C$$

Les auteurs

Les auteurs des chapitres «Logique», «Ensembles», «Arithmétique», «Nombres complexes» et «Groupes» sont :

- Arnaud Bodin (université Lille 1),
- Benjamin Boutin (université Rennes 1),
- Pascal Romon (université Marne-la-Vallée).

Les auteurs des chapitres «Nombres réels», «Suites», «Fonctions», «Dérivées» sont :

- Arnaud Bodin (université Lille 1),
- Niels Borne (université Lille 1),
- Laura Desideri (université Lille 1).

Les chapitres «Intégrales», «Développements limités», «Polynômes» sont d'Arnaud Bodin, d'après des cours de Marc Bourdon et Guoting Chen.

Les exercices en vidéos sont de Arnaud Bodin et Léa Blanc-Centi (université Lille 1).

La musique du générique est de Victor Fleurant.